Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »

Ce texte entre en vigueur le 1er avril 2017. Par application de la loi de modernisation de notre système de santé, il « décrit les modalités de gouvernance et de fonctionnement du système national des données de santé (SNDS) qui a vocation à regrouper les données de santé de l'assurance maladie obligatoire, des établissements de santé, les causes médicales de décès, les données issues des Maisons départementales des personnes handicapées ainsi qu'un échantillon de données de remboursement d'assurance maladie complémentaire ».

« Il fixe en outre la liste des organismes, établissements et services bénéficiant d'accès permanents aux données du SNDS en raison de leurs missions de service public ainsi que les modalités de ces accès. Ce texte prévoit également des possibilités d'accès ponctuel aux données du SNDS. Enfin, il prévoit l'information des personnes auxquelles les données se rapportent, et leurs droits d'accès, de rectification et d'opposition qui s'exercent auprès de la caisse d'assurance maladie dont dépend la personne ».

Consulter

• Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »
• Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé (demande d'avis n° 16018114)

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 : *Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » – APHP DAJ*

Où en est la protection de nos données personnelles avec la dernière mise à jour Windows 10 ?

Où en est la protection de nos données personnelles avec la dernière mise à jour Windows 10 ?

Quid de la confidentialité des données avec le déploiement de la mise à jour majeure Windows 10 Creators Update ? Cette nouvelle mouture de l'OS de Microsoft apporte son lot de nouvelles fonctionnalités et d'outils, avec un focus sur la création 3D, une démocratisation de la « réalité mixte » (la version de la réalité augmentée de l'éditeur), des améliorations portées à son navigateur Internet Edge…

Mais la firme de Redmond a pris les devants sur le volet de la confidentialité des données avec un meilleur contrôle via les paramètres de gestion.

Ainsi, les utilisateurs vont avoir plusieurs options pour activer ou désactiver les données de localisation, les données vocales ou les données relatives à la publicité…

Mais l'éditeur va aussi jouer la carte d'une plus grande transparence concernant les données collectées. Même s'il ne sera toujours pas possible d'effectuer un « opt out » du système de collecte de la data.

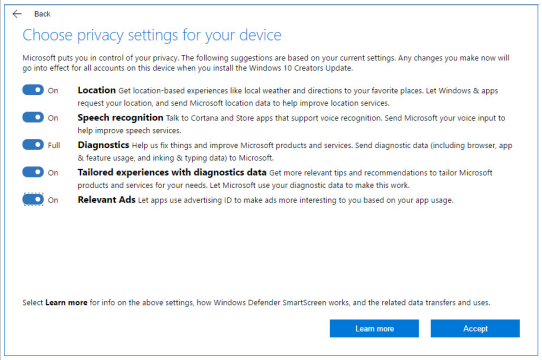
Cette transparence porte donc sur les informations qui sont collectées et la manière dont elles sont ensuite exploitées.

« Nous fournissons également un résumé détaillé des données que nous collectons auprès des utilisateurs aux niveaux de base et complet de diagnostic, » explique ainsi Microsoft dans un billet dense de blog.

En effet, la firme dirigée par Satya Nadella a décidé de réduire les options de partage des données à deux (au lieu de 3 précédemment) avec les modes « basique » et « plein ».

Selon TechCrunch, le niveau basique envoie 50% moins de données à Microsoft. Tout simplement parce que Microsoft s'est rendu compte qu'autant de données n'étaient pas nécessaires en vue d'obtenir les données de diagnostic dont elle avait besoin.

Sont aussi prévus un ensemble amélioré de descriptions sur chaque paramètre de confidentialité et une déclaration de confidentialité mise à jour…[lire la suite]



(Crédit photo : @Microsoft)

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 : *Windows 10 Creators Update : encore un effort sur la confidentialité des données – Free Tech & web*

Windows 10 : Microsoft

dévoile les données personnelles qu’il récolte

Microsoft dévoile les données personnelles que Windows 10 récolte

Un cadre haut placé chez Microsoft vient de révéler la publication d'une liste des données personnelles que l'entreprise récolte sur Windows 10. Si Microsoft tente de rassurer sur sa politique de confidentialité et la sécurisation des données, ce nouveau procédé est susceptible de relancer des débats.

Selon le site theverge.com, le chef Windows Terry Myerson explique que **Microsoft publie désormais des informations sur les données collectées** dans le cadre de Windows 10. Ces données sont publiées sur le site TechNet de Microsoft. Dans le cadre de la dernière mise à jour Creators Update et de la nouvelle politique de confidentialité, les contrôles autour des niveaux de collecte sont renforcés.

Les données personnelles : une question de sécurité des utilisateurs

Si Microsoft tente de rassurer sur les contrôles et la sécurisation des données personnelles, il n'en demeure pas moins que ses pratiques posent problème. **Microsoft est soupçonné de suivre ses utilisateurs via des traçeurs** et de ne pas respecter des choix de confidentialité exprimés par les utilisateurs Windows 10. Il y aurait danger pour le droit au respect de la vie privée. Il peut même s'agir d'espionnage.
Toutefois, les autorités de régulation veillent au grain. La France vient d'ordonner à Microsoft de cesser toute traçabilité. L'agence de protection des données de l'Union Européenne ont mis en garde contre les insuffisances des changements apportés par Microsoft Creators Update.

Le débat sur les données personnelles relancé ?

La révélation des données peut constituer une **atteinte du droit à la protection de la vie privée.** Il est tout de même légitime de se poser la question de savoir si les autorités de régulation ne protège pas certains intérêts particuliers ou si leur examen n'est pas dicté par un esprit partisan.
Après tout, Amazon, Facebook et Google sont déjà capables de repérer vos habitudes de consommation, et de vous proposer des produits en lien avec vos acquisitions passées. Même si Google a déjà pu faire l'objet d'une procédure à l'initiative de l'UE, on peut se demander pour quelles raisons, des entreprises comme Amazon, ne pourraient pas subir le même traitement que celui réservé à Google et Microsoft…[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 : *Windows 10 : Microsoft dévoile les données personnelles qu'il récolte*

Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017

	**Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017**

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.
La correspondance privée se définie comme tout message exclusivement destiné à une ou plusieurs personnes physiques ou morales, déterminées et individualisées. L'exemple le plus concret est le courriel échangé entre deux ou plusieurs correspondants, depuis un service de messagerie.
Ainsi, toute correspondance entre deux personnes doit être protégée au titre du secret, par les opérateurs dont l'activité consiste à acheminer, transmettre ou transférer le contenu de ces correspondances. Tout comme un facteur n'a pas le droit d'ouvrir un courrier postal, le fournisseur de messagerie électronique ou le fournisseur d'accès à internet sont tenus de respecter le secret des courriers électroniques.
Ce principe de confidentialité était d'ailleurs déjà garanti par l'article L32-3 du Code des postes et des communications électroniques qui prévoyait, dans sa version antérieure à la publication de la loi pour une République numérique que « *les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances* ».
La directive européenne 2002/58 modifiée relative à la vie privée dans les communications électroniques (l'article 5.1) interdit « *à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs* ».
Le contenu des communications, c'est-à-dire des correspondances entre deux individus, est par principe confidentiel et l'obligation de garantir le secret repose sur les opérateurs de télécommunication.
Il est en revanche possible de lever le secret des correspondances, en demandant aux personnes concernées leur consentement.

Qu'est-ce qui change avec la loi pour une République numérique et son décret d'application relatif à la confidentialité des correspondances ?

L'article 68 de loi pour une République numérique précise ce que couvre le secret des correspondances. Ce secret s'applique ainsi à l'identité des correspondants, au contenu, à l'intitulé et aux pièces jointes des correspondances.

Quels sont les professionnels concernés ?

Sont désormais soumis au respect du secret des correspondances, à la fois les « *opérateurs* », c'est-à-dire les opérateurs de télécommunications essentiellement, et les « *fournisseurs de services de communication au public en ligne* », en d'autres termes, tout acteur permettant à deux personnes de correspondre en ligne. Seront notamment concernés les fournisseurs de services de messagerie électronique, de réseaux sociaux, de communication synchrone (VoIP), etc.

A quelles conditions peuvent-ils exploiter la correspondance privée ?

La loi Lemaire leur permet toutefois d'exploiter la correspondance privée, **sous réserve d'obtenir le consentement des utilisateurs et pour les seules finalités suivantes** :
• l'amélioration du service de communication au public en ligne,
• la réalisation de statistiques,
• l'utilisation des données à des fins publicitaires.

Quels sont les effets en pratique pour les opérateurs de communication électronique ou fournisseurs de service ?

La CNIL rappelle que, pour être valable, ce consentement doit être libre, spécifique et informé. Il doit en outre résulter d'un acte positif et être préalable à la collecte des données, c'est-à-dire à la réalisation du traitement.

Un consentement informé

Les opérateurs souhaitant utiliser la correspondance de leurs utilisateurs à des fins statistiques, publicitaires ou encore pour améliorer leur service devront recueillir leur consentement spécifique après les avoir informés de ce qu'ils souhaitent faire (en rappelant les mentions requises par l'article 32 de la loi Informatique et libertés).

Un consentement spécifique

La CNIL rappelle que le consentement doit être spécifique et qu'à ce titre, un consentement global pour plusieurs finalités différentes, de même que l'acceptation globale des Conditions générales d'utilisation (ou CGU) du service, **ne peuvent être considérés comme un consentement valable**.

Un consentement libre

Le consentement ne doit pas être contraint, c'est-à-dire que le refus de consentir ne doit pas empêcher la personne d'accéder au service de messagerie. Le consentement doit prendre la forme d'un acte positif des utilisateurs et ne peut donc être déduit du silence ou de l'inaction des utilisateurs. Le consentement devant être recueilli avec une périodicité d'un an, la CNIL recommande que les responsables de traitement alerte les personnes dans un délai raisonnable avant l'échéance de ce délai, pour que le renouvellement ne soit pas automatique.

Un consentement renouvelé tous les ans

La loi pour une République numérique prévoit que le consentement doit être renouvelé périodiquement, c'est-à-dire recueilli tous les ans par les opérateurs exploitant les correspondances.
Par ailleurs, la CNIL rappelle que les traitements réalisés sur les correspondances doivent se limiter aux données collectées de manière loyale et licite. En conséquence, les traitements ne doivent produire des effets qu'à l'égard des personnes qui ont valablement consenti à la collecte de leurs données à caractère personnel issues du contenu de leurs correspondances. À titre d'exemple, les traitements opérés à des fins publicitaires et basés sur le contenu des correspondances ne doivent pas permettre à l'opérateur de cibler d'éventuelles personnes tierces dont les données personnelles apparaitraient dans la correspondance.
Enfin, la CNIL rappelle qu'une fois le règlement européen relatif à la protection des données, adopté, les responsables de traitement devront être en mesure de prouver que les personnes ont effectivement consenti au traitement et seront tenus de les informer de la possibilité de retirer leur consentement.

Réagissez à cet article

Source : *Secret des correspondances : un consentement renforcé des utilisateurs de services de communication électronique | CNIL*

Comment se préparer au règlement européen sur la Protection des Données Personnelles en 6 étapes ?

	**Comment se préparer au règlement européen sur la Protection des Données Personnelles en 6 étapes ?**

Le 25 mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

ETAPE 1 DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

> En savoir plus

ETAPE 2 CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

> En savoir plus

ETAPE 3 PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

> En savoir plus

ETAPE 4 GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

> En savoir plus

ETAPE 5 ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

> En savoir plus

ETAPE 6 DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

> En savoir plus

…[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

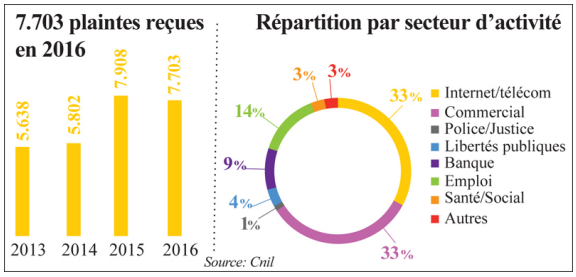
Source : *Règlement européen : se préparer en 6 étapes | CNIL*

Protection des données personnelles : Ce qui change en 2018 avec le règlement RGPD

Protection des données personnelles : Ce qui change en 2018 avec le règlement RGPD

Le nouveau règlement européen sur la protection des données personnelles entrera en vigueur le 25 mai 2018. «Ce texte rénove la régulation européenne des données et offre à l'Europe la possibilité de récupérer sa souveraineté numérique…», indique Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (Cnil).

Le règlement renforce les droits des personnes à l'ère numérique
Les entreprises doivent se préparer au nouveau cadre juridique
Entrée en vigueur en mai 2018



En 2016, la Cnil a enregistré 7.703 plaintes (un peu moins que le record de 2015, 7.900 cas). Elles ont concerné principalement les secteurs Internet/télécom et le commerce
«La complexité du règlement avec ses 99 articles et ses 200 considérants ne doit pas masquer pour autant l'essence du texte qui consiste à renforcer la place centrale de l'individu dans l'univers des données», dit-elle. Pour le cas de la France, un projet de loi devra être déposé au Parlement au plus tard en juin 2017 pour garantir une meilleure application du règlement.
■ **Nouveau cadre juridique:** Le règlement européen constitue une évolution du cadre juridique de la protection des données et permet de construire une régulation commune sur l'ensemble du territoire de l'Union. Globalement, le texte renforce l'obligation des organismes publics et privés de protéger les données personnelles de leurs utilisateurs et clients. En pratique, le droit européen s'appliquera chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet. La territorialité du droit européen se construit donc désormais autour de la personne. Cela se traduit par l'apparition de nouveaux droits (portabilité des données, limitation du traitement, réparation d'un dommage matériel ou moral…). Les obligations en matière d'information sont également renforcées notamment en cas de faille de sécurité.
■ **L'expression du consentement renforcée:** 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 ambiguë. Le but de cette évolution est d'améliorer l'information qui doit être claire et accessible aux personnes concernées par les traitements de données.
■ **Portabilité des données:** Ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme facilement réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit de redonner aux personnes la maîtrise de leurs données et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.
■ **Protection des enfants:** 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. Les Etats membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.
■ **Biométrie:** Les données biométriques doivent faire l'objet d'une vigilance particulière. Le règlement européen a consacré le caractère particulier de ces données en les qualifiant de données «sensibles», au même titre que les données concernant la santé, les opinions politiques ou les convictions religieuses, dont le traitement est par principe interdit sauf dans certains cas limitativement énumérés.
■ **Open data:** Si elle ne concerne pas initialement la protection des données à caractère personnel, le nouveau contexte numérique implique de mieux la prendre en compte. Et ce notamment au niveau de la mise à disposition des données comme de leur réutilisation, la protection de la vie privée. Le nouveau cadre juridique permet cette conciliation.
Les sanctions s'alourdissent
Les autorités de protection pourront imposer des amendes administratives (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial d'une entreprise). Ces sanctions pécuniaires pourront être prises en complément ou à la place de nombreuses mesures correctrices (ordonner de communiquer à la personne concernée une violation de données, la rectification ou encore la suspension de flux de données vers un pays tiers). Effacer des données ou limiter le traitement ou encore retirer une certification sont sur la liste des dispositions… Ces mesures et sanctions ne seront plus limitées au responsable de traitement mais pourront également être prises à l'égard d'un sous-traitant. Dans l'hypothèse de traitements transfrontaliers, la Cnil travaillera avec d'autres autorités de protection afin qu'une seule décision de sanction soit adoptée par l'autorité chef de file.
[Article original de Fatim-Zahra TOHRY]

Réagissez à cet article

Source : *Protection des données personnelles: Ce qui change | L'Economiste*

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