Règlement sur les Données Personnelles RGPD : Découvrez les coulisses de ce règlement

Règlement sur les Données Personnelles RGPD : Découvrez les coulisses de ce règlement

Depuis les couloirs du Parlement Européen, chronique de la difficile élaboration d'une nouvelle loi pour la protection des données personnelles, enjeu central opposant les citoyens aux intérêts privés.

Chaque fois que nous faisons nos courses sur Internet, interrogeons un moteur de recherche, activons la géolocalisation sur notre smartphone ou même utilisons notre carte de transport ou de crédit, nous laissons des traces : des masses d'informations personnelles sont collectées sur nos habitudes de consommation, nos goûts, nos déplacements ou nos opinions. Des informations hautement exploitables – et monnayables. Nombreux sont les observateurs à l'affirmer : les données seront le pétrole du XXIe siècle. Utilisée de manière judicieuse, cette manne offre la promesse de transformer nos vies en profondeur. Mais à quel prix ? Ces données personnelles échappent de plus en plus aux citoyens, au profit des entreprises. Comment nous protéger contre l'utilisation incontrôlée de nos données, garantir notre droit à l'autodétermination et sanctionner les contrevenants ? Selon les lobbies privés, une loi trop draconienne risquerait de faire fuir les entreprises du territoire européen. Mais faut-il pour autant sacrifier la vie privée des citoyens ?

Loi à réformer
Depuis plusieurs années, l'Union européenne travaille à réformer la loi sur la protection des données personnelles. Le jeune député vert européen Jan Philipp Albrecht a notamment pris ce combat à bras-le-corps, en se faisant le rapporteur du Parlement européen sur la réglementation de la protection des données. Ce documentaire suit le parcours complexe de la législation européenne en la matière, en interrogeant des acteurs aux intérêts souvent divergents : politiques, juristes, membres de la société civile ou du monde des affaires.
.

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

Sur la Protection des données personnelles, les programmes d’Emmanuel Macron et Marine Le Pen sont plutôt faibles

Sur la Protection des données personnelles, les programmes d’Emmanuel Macron et Marine Le Pen sont plutôt faibles

Emmanuel Macron et Marine Le Pen présentent tous les deux des programmes numériques assez parcellaires. On fait le point.

Sur la question de la vie privée des internautes, **Marine Le Pen** propose de « créer une charte à valeur constitutionnelle de protection des données personnelles », sans jamais préciser ce qu'une telle charte pourrait induire pour les citoyens. La candidate frontiste souhaite également mettre en place l'obligation « de stocker les données personnelles des Français sur des serveurs hébergés en France », sans toutefois livrer plus de détails sur les modalités techniques de telles mesures. Seule véritable proposition concrète dans ce dossier : la création de la carte unique biométrique, qu'elle aimerait étendre à la carte vitale afin de lutter contre la fraude, et l'obligation pour les entreprises de sotcker en France les données personnelles des citoyens français.

Emmanuel Macron, lui, reste tout autant vague. Il souhaite « développer les instruments d'une transparence sur l'usage des données privées par les acteurs du numérique« , mais ne dit pas lesquels. On retrouve le même flou lorsqu'il propos de « bâtir des murailles » et « patouiller dans le cyberespace » pour faire de la cybersécurité, « une priorité de la sécurité nationale ». L'ancien ministre de l'Économie et des finances va même jusqu'à proposer »une banque de données numériques réutilisables : « Dans le respect de la vie privée et du secret des affaires, les administrations qui délivrent des licences (par exemple pour les hôtels) devront mettre à disposition leurs données. Face aux géants étrangers, des nouvelles start-up pourront ainsi s'adresser par exemple à tous les hôteliers pour leur offrir une alternative aux services existants ». Et l'ancien banquier d'affaires français de suggérer également « un service public numérique de la justice », avec portail unique d'accès : « Les citoyens et leurs avocats y trouveront toutes les informations pratiques et la jurisprudence applicable à leur cas. Ils pourront se pourvoir en justice depuis leur ordinateur, transmettre une requête, des pièces, ou suivre leur dossier depuis leur smartphone ». Il aimerait également renégocier le « Privacy Shield » d'ici 2018 et créer une « agence européenne pour la confiance numérique » qui serait « chargée de réguler les grandes plateformes numériques »…[lire la suite]

Réagissez à cet article

Source : *Sur le numérique, les programmes d'Emmanuel Macron et Marine Le Pen sont plutôt faibles*

Allocab condamné par la Cnil

Allocab condamné par la Cnil

La police de protection des données personnelles en ligne vient de condamner la société Allocab à verser une amende de 15 000 euros. L'entreprise de VTC aurait mal protégé et conservé certaines données bancaires de ses utilisateurs sans tenir compte des avertissements de la Cnil, dont le verdict est tombé ce 25 avril.

Les données des utilisateurs frauduleusement conservées

La société de VTC (Voiture avec chauffeur) Allocab propose des chauffeurs privés aux utilisateurs de son application. En réponse aux demandes des clients, la Cnil (Commission nationale de l'informatique et des libertés) a effectué un contrôle des activités de la firme dans le cadre de la loi « Informatique et Libertés ». L'enquête a révélé qu'Allocab commettait plusieurs manquements à ce texte : elle rapporte notamment que « des données relatives à des comptes inactifs et des cryptogrammes de cartes bancaires étaient encore présents dans le système d'information et la sécurité des données n'était pas suffisamment assurée » et que les mots de passe à un seul caractère étaient par ailleurs admis, ce qui ne garantit aucune sécurité aux données des utilisateurs. Il ne s'agit pourtant pas du premier faux pas de cette entreprise, déjà sanctionnée en 2015.

Des avertissements ignorés

Le 10 novembre 2015, Allocab se voyait mise en demeure par la Cnil suite à la plainte d'un utilisateur. L'institution ordonnait à l'entreprise de détruire les données des anciens clients et de « prendre toute mesure nécessaire pour garantir la sécurité et la confidentialité des données des utilisateurs du site », notamment en limitant la durée de conservation des cryptogrammes de cartes bancaires et de toutes les données des utilisateurs. Suite à cette première condamnation s'est déroulée une longue correspondance dans laquelle Allocab prétextait des dysfonctionnements techniques et certifiait mettre en place des mesures nécessaires. Ces affirmations ont incité la Cnil à mener un deuxième contrôle. Au cours de cette seconde investigation fin 2016, elle découvre que plusieurs de ses injonctions ne sont pas respectées : de nombreux comptes inactifs existent encore sur la plateforme, tout comme les données et cryptogrammes des cartes bancaires de nombreux utilisateurs.

15 000 euros d'amende

Les fameux dysfonctionnements invoqués par Allocab n'ont pas convaincu la commission, dont un comité restreint l'a condamné le 13 avril dernier au versement d'une amende de 15 000 euros…[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 : *Allocab condamné par la Cnil*

Les données de santé des Français désormais en libre accès

Les données de santé des Français désormais en libre accès

Dans un communiqué du 10 avril 2017, le gouvernement a indiqué qu'il ouvrait l'accès aux données issues du Système national des données de santé (SNDS) aux organismes exerçant une mission de service public pour toute étude, recherche et évaluation présentant un intérêt public. Ces organismes peuvent désormais consulter et exploiter les données du SNDS suivant certaines conditions détaillées dans le décret du 26 décembre 2016.

Ainsi, comme le précise le gouvernement :

• L'État, l'Assurance maladie, l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), la Haute Autorité de santé (HAS) ou encore Santé publique France peuvent accéder aux données du SNDS de manière permanente pour leur permettre d'assumer leurs missions

• Les équipes de recherche des centres hospitaliers universitaires (CHU), de l'Institut national de la santé et de la recherche médicale (INSERM) et des centres de lutte contre le cancer peuvent désormais consulter l'échantillon correspondant à 1/100ème de la population.

• Les autres organismes publics ou privés, à but lucratif ou non lucratif, auront eux aussi prochainement accès aux données issues de cette base pour toute étude, recherche et évaluation présentant un intérêt public. Ils seront, eux-aussi, soumis aux conditions précisées dans le décret du 26 décembre 2016

La loi interdit l'usage de ces informations pour deux finalités :

• La promotion commerciale des produits d'assurance santé

• La modulation des contrats d'assurance santé (évolution des primes, exclusions,…

Toutefois, cette annonce suscite des craintes et la réprobation, notamment chez certains acteurs de la santé.

Ainsi, la Fédération des Médecins de France – syndicat qui regroupe près de 3000 adhérents – s'oppose à cette mesure. *« Si la loi autorise des accès à cette vaste base de données au nom de la recherche et annonce la future possibilité à des entreprises lucratives de pouvoir y accéder également, la FMF rappelle que les données du SNDS ne seront pas anonymisées mais seulement pseudonymisées avec une possibilité d'identification. »* explique le syndicat dans un communiqué.

La FMF alerte :

– du risque élevé de perte de confidentialité de leurs données personnelles, soit en raison du piratage, soit en raison du nombre élevé de personnes potentiellement concernées par l'accès aux données du SNDS. La CNIL elle-même a estimé que « le niveau de sécurité envisagé ne sera pas atteint au lancement du traitement SNDS en mars 2017 »[1]. Bien que la loi prévoie un agrément très sévère pour les hébergeurs de données de santé, les mini serveurs de données, de radiologie ou de biologie, permettant un accès rapide aux résultats, ne sont pas tous agréés, et leur accès est très modérément protégé...[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 : *Les données de santé des Français désormais en accès libre –*

Protection des données : ce qui va changer pour les entreprises en 2018

Protection des données : ce qui va changer pour les entreprises en 2018

En mai 2018, un règlement européen va entraîner d'importants changements dans la pratique des entreprises en matière de gestion des données personnelles. En quoi consistent ces changements et comment s'y préparer ?

Protection des données : ce que prévoit le règlement européen de 2016

Contrairement à une directive, le règlement européen, adopté en 2016, est directement applicable dans l'ensemble de l'Union européenne sans nécessiter de transposition dans les différents Etats membres et ce à partir du 25 mai 2018. Il concerne toutes les entreprises utilisant des données personnelles.
Ainsi, à cette date, les responsables de traitement devront s'être mis en conformité avec le règlement sous peine de sanctions.

Principal changement :
Ce règlement marque le passage d'une logique de « formalités préalables » (déclarations, autorisations) à une logique de « conformité » dont les acteurs seront responsables sous le contrôle du régulateur (la CNIL en France). Ainsi, les responsables de traitements de données n'auront plus à effectuer de déclarations à la CNIL dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.
Par contre, ils devront d'entrée mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »). Ils devront également être capables de démontrer cette conformité à tout moment.

	Pour les traitements à risque, il faudra toutefois conduire une étude d'impact complète faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Cela concerne notamment les données sensibles qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi les données génétiques ou biométriques. En cas de risque élevé, il faudra consulter la CNIL avant de mettre en œuvre ce traitement, cette dernière pouvant décider de s'y opposer.

Ce règlement renforce par ailleurs les droits des personnes. En effet, chaque personne concernée par les traitements de données va avoir le droit à la mise à disposition d'une information claire, intelligible et aisément accessible et va devoir donner son accord pour le traitement des données. La preuve de ce consentement incombant au responsable de traitement.

Protection des données : mise en place des délégués à la protection des données

Le règlement européen instaure des délégués à la protection des données (DPD). Ce seront les successeurs des correspondants informatique et libertés (CIL) dont plus de 17 700 organismes sont d'ores et déjà dotés en France et dont la mise en place permet de se dispenser de certaines déclarations.
A la différence du CIL, dont la désignation est actuellement optionnelle, la désignation du DPD est obligatoire dans le secteur public et pour les responsables de traitement et les sous-traitants dont les activités principales les amènent :
• à réaliser un suivi régulier et systématique des personnes à grande échelle ;
• à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.
Pour les autres, leur désignation est facultative…[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 : *Protection des données : ce qui va changer pour les entreprises – Editions Tissot*

Est-ce que Linky aspire nos données personnelles ?

Est-ce que Linky aspire nos données personnelles ?

Linky, un compteur qui ne vous veut pas que du bien ! Ce boitier qui doit être installé dans tous les foyers relèvera en direct et à distance vos habitudes de consommation d'électricité.

Par ailleurs, des incidents ont lieu lors de la pose de ces compteurs, notamment lorsque des personnes s'y opposent : à Plouha et dans sa région récemment, plusieurs incidents ont été constatés, avec notamment une dame de 73 ans bousculée par un installateur alors qu'elle s'opposait à l'installation.
Avec le prétexte d'établir une facture plus précise, EDF prévoit de remplacer 90% des anciens compteurs en 4 ans. Un changement qui suscite de vives polémiques. En effet, de nombreuses communes s'opposent à l'installation de ce compteur dit intelligent. Si l'efficacité et le risque de surcoût sont remis en question, la menace d'intrusion dans la vie privée est également pointée du doigt.
En effet, par son système de collecte de données à distance, le compteur Linky est un véritable concentré d'informations personnelles. Il est techniquement capable de recueillir les index journaliers et la courbe de charge, c'est-à-dire un relevé précis de la consommation électrique de l'utilisateur. Ces données permettent de déduire des informations sur les habitudes de vie des consommateurs.
Des millions de Français seront concernés et des millions de données personnelles seront stockées par ERDF, qui souhaite entrer dans la danse du commerce d'informations, le Big Data. Pas étonnant, car cette mine d'or peut rapporter très gros. En effet, elle fait l'objet d'un véritable business, estimé à plusieurs milliers de milliards d'euros…[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 : *Linky, vendeur de données personnelles –*

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.

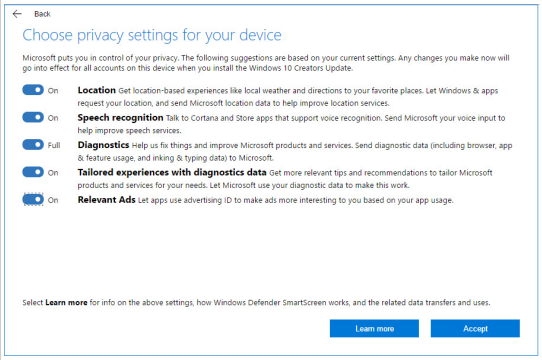
Cette transparence porte donc sur les informations qui sont collectées et la manière dont elles sont ensuite exploitées.

« 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*