iCloud indiscret sur nos journaux d’appels…

iCloud indiscret sur nos journaux d’appels…

La synchronisation iCloud envoie sur les serveurs d'Apple le journal des appels d'un appareil sous iOS, en remontant jusqu'à quatre mois. Une option sur laquelle l'utilisateur ne peut pas influer directement et qui nécessite une désactivation complète d'iCloud Drive pour être coupée. Pour la société, il ne s'agit que de simplifier la vie des clients.

iCloud, quand il est actif sur un appareil Apple, synchronise et sauvegarde de nombreux éléments : contacts, agendas, messages, réglages et ainsi de suite. L'idée est de simplifier la vie de l'utilisateur s'il vient à perdre son appareil ou tout simplement s'il en utilise plusieurs. La « réserve » de données est ainsi la même et il ne s'embarrasse pas de doublons et autres.

Une synchronisation active, même quand la sauvegarde iCloud est coupée

Mais iCloud synchronise aussi le journal des appels, ce qui n'est en fait mentionné nulle part. La découverte a été faite par Elcomsoft, à qui l'on doit déjà les révélations sur la fragilité du chiffrement dans les sauvegardes faites par iOS 10. Toutes les informations du journal d'appel sont présentes : les appels classiques émis et reçus, les appels FaceTime, et globalement tout ce qui peut y inscrire des évènements depuis iOS, comme Skype et WhatsApp.

Selon Elcomsoft, la seule manière de couper cette synchronisation, qui remonte le journal jusqu'à quatre mois en arrière, est de désactiver complètement iCloud Drive, un choix que l'on trouve dans les options du service dans iOS et macOS. Désactiver iCloud lui-même ne suffit pas.

Mais ce faisant, d'autres services peuvent ne plus fonctionner. WhatsApp, justement, se sert de Drive pour stocker ses sauvegardes. D'autres applications l'utilisent pour entreposer leurs documents et les synchroniser entre les machines de l'utilisateur. Il reste bien entendu le cas où cette révélation ne dérange pas l'utilisateur.

Une commodité, et pas seulement pour les utilisateurs

Pour Apple, il n'y a pas vraiment de problème, comme la firme l'a indiqué à *Forbes* : « *Nous offrons la synchronisation du journal d'appels comme une commodité à nos clients, pour qu'ils puissent rappeler depuis n'importe lequel de leurs appareils.* […]*L'accès aux données iCloud – y compris les sauvegardes – requiert l'identifiant Apple et le mot de passe. Nous recommandons à tous nos clients de choisir des mots de passe forts et d'utiliser l'authentification à deux facteurs* ».

Tout irait bien donc à partir du moment où le mot de passe serait assez fort. Cependant, ce n'est pas aussi simple. L'affaire de l'iPhone 5c a certes montré qu'Apple ne pouvait pas déverrouiller par la force un appareil et récupérer les données (le code de verrouillage participe à la clé de chiffrement), mais iCloud, même s'il communique de manière chiffrée, dépose des données sur les serveurs de l'entreprise.

Or, comme pour iMessage, ces données sont disponibles sur demandes si les forces de l'ordre les réclament, dument armées d'un mandat. Une situation similaire à ce que l'on retrouve dans le domaine de la téléphonie mobile « classique » depuis des années.

L'expert Jonathan Zdziarski, interrogé par Forbes, a indiqué que rien n'empêchait en théorie Apple de basculer dans le chiffrement intégral pour l'ensemble de ses services. « *Mais d'un point de vue politique* » ajoute-t-il, « *cela pourrait déclencher une guerre avec certaines agences fédérales qui utilisent ces données quotidiennement* ». Une situation à ce qu'on a pu voir avec WhatsApp lors de son passage au chiffrement de bout-en-bout.

Original de l'article mis en page : Apple : iCloud synchronise sans accord les journaux d'appels

DNS et GDPR, ou quand sécurité et réglementation se retrouvent

DNS et GDPR, ou quand sécurité et réglementation se retrouvent

Le nouveau GDPR (Règlement général sur la protection des données) est un règlement de l'Union européenne qui vise à renforcer la protection des données dans tous les Etats membres de l'UE, en remplacement de la Directive 95/46/CE de 1995.…[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

Intervention de la CNIL à l'encontre du site Alainjuppe2017

Intervention de la CNIL à l'encontre du site Alainjuppe2017

La CNIL intervient pour faire corriger une fuite de données concernant le site Internet de l'ancien candidat aux présidentielles françaises, alainjuppe2017.fr.

L'information est restée confidentielle le temps des primaires de la droite. Il fallait surtout que la faille concernée soit corrigée et la fuite en résultant bouchée. Il y a quelques jours, un internaute anonyme a fait appel au protocole d'alerte de ZATAZ pour faire corriger un bug qui permettait en quelques clics de souris d'accéder à plus de 20.000 profils d'internautes inscrits sur le site alainjuppe2017.fr.
Une porte ouverte présidentielle possible en raison d'un oubli interne. L'un des gestionnaires de l'espace politique avait oublié… de retirer le debug du site ! Bilan, la moindre erreur dans l'espace numérique de soutien à Alain Juppé, via l'espace « Mobilisation », permettait d'accéder à des informations privées et sensibles !…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : ZATAZ Protocole d'alerte ZATAZ : intervention de la CNIL à l'encontre du site Alainjuppe2017 – ZATAZ

Forum sur les donneés personnelles au Sénégal

	Forum sur les donneés personnelles au Sénégal

La Commission de protection des données personnelles, en partenariat avec le cabinet Futurs choisis a organisé, jeudi, un forum de sensibilisation à l'intention de certains corps de métier. La rencontre a permis d'échanger et de communiquer en langue nationale sur l'intérêt de protéger ses informations personnelles face aux risques multiples : évolution des technologies, atteintes à la vie privé sur les réseaux sociaux et installation tous azimuts de vidéos surveillances.

Forte de sa mission de communication et sensibilisation, la Commission des données personnelles (Cdp) a pris l'initiative de rencontrer, jeudi, certains corps de métier évoluant surtout dans le secteur informel, notamment les commerçants, pour échanger avec eux, en langue wolof, sur la loi sur les protections de données personnelles, des missions de la Cdp, l'importance de la protection des données personnelles, etc.
Le séminaire a été également une occasion pour la présidente de la Cdp, Awa Ndiaye, de revenir sur les multiples atteintes à la vie privée enregistrées par la commission et relatives aux réseaux sociaux et à l'installation de caméras de surveillance dans certaines entreprises privées.
L'équipe du cabinet Futurs choisis a présenté, en langue wolof, à l'assistance, les missions et le rôle de la Commission de protection des données personnelles non sans préciser l'intérêt de protéger ses données personnelles que Pr Abdoullah Cissé a même qualifié de « sutura » en wolof. Pour lui, en un moment de l'histoire, on pouvait se fier à quelqu'un tout en ayant la certitude que le secret pouvait être gardé. Mais, avec la floraison des nouvelles technologies de l'information et de la communication, cette ère est révolue. D'où l'intérêt, pour lui, de protéger ses données personnelles pour ne pas être victime de diffamation, d'escroquerie, comme il est constaté de plus en plus sur les réseaux sociaux.

Atteintes à la vie privée
La présidente de la Cdp s'est aussi exprimée sur l'installation tous azimus de caméras et vidéosurveillances. Selon elle, de plus en plus de commerçants installent dans les marchés des caméras de surveillance sans compter les domiciles et entreprises privés qui s'y mettent aussi. Pour Mme Ndiaye, cette installation n'est pas interdite parce que chacun a le droit de se préoccuper de sa sécurité. Toutefois, la présidente demande à ce que les détenteurs de ces caméras de surveillance se mettent en règle par rapport à la loi pour la protection des données à caractère personnel qui régule toute la vidéosurveillance.
« Les détenteurs de caméras de surveillance doivent se mettre en règle avec la loi en déclarant ces vidéosurveillances auprès de la Cdp avant de les installer car ils ne doivent pas être installées n'importe où, surtout dans le cadre du travail, dans les entreprises privées », indique-t-elle. A l'en croire, ils ont eu des cas d'ouvriers qui se sont indignés d'être sous caméras vidéosurveillance 24 h/24h alors que la loi l'interdit et prévoit même des sanctions d'ordre administratives voire pénales.
Les atteintes à la vie privée sur les réseaux sociaux ont été également abordées lors de ce séminaire. En ce sens, renseigne la présidente de la Cdp, au total, ils ont reçu 200 plaintes depuis que la Commission existe, et ce nombre ne cesse d'augmenter non pas à cause de l'installation de vidéosurveillances, mais par rapport aux réseaux sociaux.
« De plus en plus de personnes se voient menacées dans leur intégrité et leur vie privée. Ces derniers n'hésitent pas à se rapprocher de la Cdp pour faire effacer certaines de leurs données qui ont été diffusées de façon illicite », informe-t-elle.
Par Maguette Guèye DIEDHIOU

Réagissez à cet article

Original de l’article mis en page : Le Soleil – Forum sur les donneés personnelles : La Cdp sensibilise le grand public en wolof

---

La loi pour une République numérique protège encore plus nos données personnelles

La loi pour une République numérique protège encore plus nos données personnelles

---

Quels sont les apports de la loi république numérique en matière de protection des données personnelles ?

La loi pour une République numérique du 7 octobre 2016 crée de nouveaux droits informatique et libertés et permet ainsi aux individus de mieux maîtriser leurs données personnelles. Elle renforce les pouvoirs de sanctions de la CNIL et lui confie de nouvelles missions. Elle contribue également à une meilleure ouverture des données publiques.
Certaines dispositions anticipent le règlement européen sur la protection des données personnelles applicable en mai 2018.
Publiée au Journal Officiel du 8 octobre 2016, la loi pour une république numérique introduit de nombreuses dispositions directement applicables, d'autres doivent attendre la publication de décrets d'application. Nous recensons ci-dessous les dispositions d'application directe. Ce recensement sera mis à jour au fur et à mesure de la publication des décrets d'application.

De nouveaux droits pour les personnes

L'affirmation du principe de la maîtrise par l'individu de ses données
Le droit à l'autodétermination informationnelle s'inspire d'un droit similaire dégagé par la juridiction constitutionnelle allemande. Il renforce positivement les principes énoncés à l'article 1er de la loi Informatique et Libertés en affirmant la nécessaire maîtrise de l'individu sur ses données.

Le droit à l'oubli pour les mineurs
L'article 40 de la loi Informatique et libertés prévoit désormais un « droit à l'oubli » spécifique aux mineurs et **une procédure accélérée pour l'exercice de ce droit**. Lorsque la personne concernée était mineure au moment de la collecte des données, elle peut obtenir auprès des plateformes l'effacement des données problématiques « dans les meilleurs délais ».
En l'absence de réponse ou de réponse négative de la plateforme dans un délai de un mois, la personne peut saisir la CNIL qui dispose alors d'un délai de 3 semaines pour y répondre.

La possibilité d'organiser le sort de ses données personnelles après la mort
Le nouvel article 40-1 de la loi Informatique et libertés permet aux personnes de donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.
Une personne peut être désignée pour exécuter ces directives. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés.
Ces directives sont :
• générales, lorsqu'elles portent sur l'ensemble des données concernant une personne ;
• ou particulières, lorsque ces directives ne concernent que certains traitements de données spécifiques.

Lorsque ces directives sont générales et portent sur l'ensemble des données du défunt, elles peuvent être confiées à un tiers de confiance certifié par la CNIL.

Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées aux responsables de traitement (réseaux sociaux, messagerie en ligne) en cas de décès. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.
En l'absence de directives données de son vivant par la personne, les héritiers auront la possibilité d'exercer certains droits, en particulier :
1. le droit d'accès, s'il est nécessaire pour le règlement de la succession du défunt ;
2. le droit d'opposition pour procéder à la clôture des comptes utilisateurs du défunt et s'opposer au traitement de leurs données.

La possibilité d'exercer ses droits par voie électronique
Le nouvel article 43 bis de la loi Informatique et Libertés impose, « lorsque cela est possible », de permettre à toute personne l'exercice des droits d'accès, de rectification ou d'opposition par voie électronique, si le responsable du traitement des données les a collectées par ce vecteur.

Plus d'information et de transparence sur le traitement des données.

L'information des personnes sur la durée de conservation de leurs données
L'obligation d'information prévue par l'article 32 de la loi Informatique et Libertés est renforcée. Les responsables de traitements de données doivent désormais informer les personnes de la durée de conservation des données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

Les compétences de la CNIL confortées et élargies

Un pouvoir de sanction renforcé
Le plafond maximal des sanctions de la CNIL **passe de 150.000€ à 3 millions €** (anticipation sur l'augmentation du plafond du montant des sanctions par le règlement européen qui sera applicable le 25 mai 2018 et prévoit un plafond pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial).
La formation restreinte de la CNIL peut désormais ordonner que les organismes sanctionnés informent individuellement de cette sanction et à leur frais, chacune des personnes concernées.
Elle pourra également prononcer des sanctions financières sans mise en demeure préalable des organismes lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité.

Une consultation plus systématique de la CNIL.
La CNIL sera saisie pour avis sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Cette rédaction permettra à la CNIL d'apporter son expertise aux pouvoirs publics de manière plus systématique, alors que les textes actuels ne prévoient sa saisine que sur les dispositions relatives à la « protection » des données personnelles.

La publicité automatique des avis de la CNIL sur les projets de loi.
Cette disposition renforce la transparence sur les avis de la CNIL.

De nouvelles missions :
• **L'affirmation de sa mission de promotion de l'utilisation des technologies protectrices de la vie privée**, notamment les technologies de chiffrement des données.
• **La certification de la conformité des processus d'anonymisation** des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation. L'anonymisation des bases de données est une condition essentielle à leur ouverture ou à leur partage : elle permet de prémunir les personnes des risques de ré-identification, et les acteurs (administrations émettrices de données, ré-utilisateurs, entreprises privées qui réalisent des recherches notamment statistiques), de la mise en cause de leur responsabilité en la matière. La certification ou l'homologation de méthodologies d'anonymisation ainsi que la publication de référentiels ou de méthodologies générales par la CNIL sera ainsi un gage de protection des personnes et de sécurité juridique pour les acteurs.
• **La conduite par la CNIL d'une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques.** Même si la loi Informatique et Libertés a toujours comporté une dimension éthique fondamentale, comme en témoignent tant ses conditions de création et son article 1er, que la composition de la Commission, la révolution numérique implique une réflexion élargie sur sa dimension éthique.

L'ouverture des données publiques étendue

La loi pour une république numérique ne remet pas en cause l'équilibre entre transparence administrative et protection de la vie privée et des données personnelles. En effet, les critères de communicabilité n'ont pas changé, et la publication – donc la réutilisation – est subordonnée au caractère librement communicable du document.
Pour autant, en passant d'une logique de la demande d'un accès à une logique de l'offre de données publiques, la loi vise clairement à ouvrir très largement les données publiques. La CNIL va accompagner cette ouverture, notamment en répondant aux demandes de conseil des collectivités publiques ou des réutilisateurs, puisque toute réutilisation de données personnelles est soumise au « droit commun » Informatique et Libertés. La possibilité pour la CNIL d'homologuer des méthodologies d'anonymisation constituera un élément important de cette régulation.
En matière de gouvernance de la donnée, la loi prévoit un rapprochement entre la CNIL et la CADA, à travers, notamment, une participation croisée dans les deux collèges.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et 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).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l’article mis en page : Ce que change la loi pour une République numérique pour la protection des données personnelles | CNIL

La Russie bloque le réseau social LinkedIn

La Russie bloque le réseau social LinkedIn

En bloquant le réseau social professionnel, la Russie vient de démontrer à tous les géants du web qui ne respecteraient pas sa législation, le sort qui les attends. Le pays impose la localisation des données personnelles des utilisateurs nationaux dans le pays.…[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

Comment être en conformité au Règlement sur les Données Personnelles dans les temps ?

Comment être en conformité au Règlement sur les Données Personnelles dans les temps ?

Conformité au GDPR : comment être dans les temps ?

Nous le savons tous, la transformation numérique a bouleversé et continue de bouleverser notre quotidien, nos modèles économiques et modifie nos échelles de temps. On ne parle plus que d'instantanéité, de prédiction et d'anticipation. Les technologies permettent de disposer de millions de « données consommateur », de les exploiter dans l'instant, et ainsi inciter à tel achat ou tel comportement. Ces données, nous les fournissons d'ailleurs volontairement ou involontairement à travers l'utilisation quotidienne de nos smartphones, tablettes, ordinateurs et de plus en plus d'objets connectés de toutes sortes.
Mais que se passe-t-il si ces données, nos données, sont dérobées et exploitées ? Les conséquences peuvent être dévastatrices…tant pour le consommateur que pour l'entité qui les détient.
Le GDPR, nouveau règlement européen, a notamment pour ambition de faire prendre conscience aux entreprises de la valeur des données personnelles et de les responsabiliser quant à leur utilisation et donc à leur protection…

Seulement deux ans pour se mettre en conformité
Même si la protection des données n'est qu'un volet d'un texte qui en comporte beaucoup d'autres (droit à l'oubli, portabilité des données, gestion des consentements…), en mai 2018, toute entreprise devra être en mesure de prouver à n'importe quel moment, que les données personnelles qu'elle détient (IBAN, numéros de téléphone, identifiants divers, etc.) sont protégées et surtout inexploitables en cas de vol. Le texte préconise à cet effet la « pseudonymisation » des données (c'est-à-dire les « anonymiser » de manière réversible) afin de garantir l'impossibilité de leur utilisation en cas de vol.

Pseudonymiser les données : le challenge d'y arriver seul
Outre la complexité et le coût du développement d'une technologie permettant d'anonymiser les données, la conformité au GDPR a des impacts techniques, organisationnels et juridiques importants, ne serait-ce « que » pour la gestion des consentements et le droit à l'oubli. Il faut répertorier les données, mesurer leur degré de sensibilité, mettre en œuvre des techniques permettant le niveau de protection correspondant à la finalité de leur traitement, etc. Tout ceci va bien sûr engendrer des charges importantes pour les DSI. Partir de zéro avec un délai de deux ans pour réussir est un challenge que seules les entreprises avec une DSI disponible vont pouvoir relever. Une DSI disponible ? Elle est déjà bien occupée à développer de nouveaux services, de nouvelles applications. C'est pourquoi, se reposer sur des outils et des services qui sont capables depuis des années de protéger des données sensibles de paiement en réalisant des centaines de millions d'opérations de tokenisation / dé-tokenisation par mois semble être une solution à privilégier…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et 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).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : Conformité au GDPR : comment être dans les temps ? – Global Security Mag Online

Interrogation des entreprises sur le Règlement européen sur la protection des données

Interrogation des entreprises sur le règlement européen sur la protection des données

Les entreprises veulent obtenir de la CNIL et du G29 des clarifications sur la responsabilité du délégué à la protection des données (DPO).

La Commission nationale de l'informatique et des libertés (CNIL) a rendu publique lundi la synthèse de contributions proposées lors d'une consultation sur le Règlement européen sur la protection des données (RGPD ou GDPR, en anglais). Rappelons que ce Règlement, qui entrera en vigueur en mai 2018, introduit de nouveaux droits des personnes et des obligations nouvelles pour les entreprises. Le texte renforce également les sanctions administratives à l'encontre des responsables de traitement et des sous-traitants qui ne respecteraient pas les dispositions du texte. Les entreprises et les administrations actives dans l'Union européenne sont toutes concernées, et pas seulement celles qui ont adopté le Cloud. Les professionnels ont été consultés cet été par la CNIL.

225 contributeurs, entreprises et fédérations professionnelles, ont posté plus de 540 contributions, soumises à 994 votes. Quatre premiers thèmes inscrits au plan d'action du G29, le groupe des CNIL européennes, ont été abordés. La mission de délégué à la protection des données inquiète le plus.

CIL, de futurs DPO ?

Un délégué à la protection des données (DPO) est-il responsable pénalement ? Peut-il être licencié pour faute ? Pourra-t-il exercer une autre fonction ? Les interrogations des entreprises sont nombreuses. Elles attendent des clarifications sur la responsabilité, le rôle, les moyens et les missions de ce DPO, qui n'est pas sans rappeler le CIL (correspondant informatique et libertés).

Pour répondre à ces attentes, la CNIL se dit prête à réaliser *« des actions de communication auprès des organismes ayant actuellement un CIL, et auprès des fédérations professionnelles concernées par la désignation obligatoire d'un DPO (courriers spécifiques, fiches pratiques) »*. Par ailleurs, les ateliers CIL seront enrichis (format, volume et contenus), a fait savoir le régulateur français.

Selon les prévisions de l'IAPP (International Association of Privacy Professionals), 75 000 postes de DPO seront à pourvoir dans le monde, dont au moins 28 000 en Europe et aux États-Unis. Le but : répondre présent dès le lancement du Règlement européen sur la protection des données.

Portabilité mal perçue

Le droit à la portabilité permet à une personne de récupérer des données à caractère personnel, sous une forme aisément réutilisable, et, si elle le souhaite, de les transférer à un tiers. Les entreprises y voient l'occasion de *« redonner confiance au client dans l'exploitation qu'elles font de ses données »*. Mais elles s'interrogent aussi beaucoup sur le coût et le périmètre réel de ce nouveau droit, qu'elles souhaitent *« limiter au strict minimum »*, selon la CNIL.

Le groupe technologie du G29, de son côté, planche sur un avis visant à clarifier ce périmètre, *« en fonction duquel les actions à mettre en oeuvre pourront être définies »*. À préciser, par conséquent.

Certification et labellisation

Le Règlement européen encourage aussi la mise en place de mécanismes de certification et de labels de protection des données. La délivrance de ces labels pourra être réalisée par le régulateur ou des organismes de certification accrédités. Les entreprises y sont plutôt favorables, à la condition que le cadre européen garantisse *« un niveau élevé et homogène des normes utilisées »*. Et les PME ne veulent pas de processus coûteux et complexes de certification ou labellisation. Les attentes des CIL, organismes et fédérations professionnelles sont fortes dans ce domaine. La CNIL, en plus d'actions déjà menées à leur attention, leur proposera de nouveaux supports et outils didactiques…[lire la suite]

Original de l'article mis en page : Règlement européen sur la protection des données : les entreprises s'interrogent

Contrôles biométriques en entreprise : vos obligations changent !

	Contrôles biométriques en entreprise : vos obligations changent !

Le cadre légal régissant la mise en place de dispositifs biométriques en entreprise évolue. En effet, la Cnil a adopté le 30 juin 2016, suite aux exigences fixées par le règlement européen sur la protection des données personnelles (2), 2 autorisations uniques, publiées au journal officiel le 27 septembre 2016.

Ces autorisations uniques fixent un nouveau cadre légal afin d'encadrer le recours aux dispositifs biométriques et protéger au mieux les libertés individuelles des personnes concernées par de tels systèmes d'identification.
Ainsi, les entreprises ayant recours à la mise en place de dispositifs biométriques ne seront plus soumises à une autorisation préalable de la Cnil. Elles devront simplement réaliser une demande d'autorisation unique et se conformer aux obligations prévues par l'autorisation.

La Cnil distingue désormais 2 types de dispositifs :
1/ l'autorisation unique 052 (3) pour les dispositifs garantissant la maîtrise par la personne concernée sur son gabarit biométrique. Ce peut être soit :
– un système recourant au stockage des données biométriques sur un support individuel détenu par les personnes concernées ;
– si la détention d'un support dédié au seul stockage du gabarit n'est pas adaptée à l'architecture et au contexte d'exploitation du dispositif, le responsable du traitement peut, de manière alternative, assurer le verrouillage des données biométriques stockées en base, par un secret détenu uniquement par la personne concernée ;
Dans ces deux hypothèses, l'utilisation du gabarit biométrique est conditionnée à une action de la personne concernée en tant que détentrice du gabarit ou du secret permettant de le déverrouiller.

2/ l'autorisation unique 053 (4) pour les dispositifs reposant sur une conservation des gabarits en base par le responsable du traitement.
Un « gabarit » biométrique désigne les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques, biologiques ou comportementales de la personne concernée.

Ainsi, à chaque demande d'autorisation unique visant à mettre en place un dispositif biométrique dans leur entreprise, les dirigeants doivent se conformer à certaines exigences :
• justifier de la nécessité et de la pertinence d'avoir recours à un dispositif biométrique. Le recours à ce dernier ne doit pas avoir pour effet de se substituer à des dispositifs non biométriques ;
privilégier les dispositifs biométriques qui garantissent aux personnes concernées la maîtrise de leur gabarit ;
justifier et garantir la protection et la conservation des gabarits en base ;
• prendre toute mesure permettant de limiter les risques d'atteinte à la vie privée.
Si vous avez mis en place un dispositif biométrique sous couvert de l'ancien cadre légal, vous devez vérifier s'il répond à ces nouvelles exigences :
si c'est le cas : un engagement de conformité à l'une de ces nouvelles autorisations peut être réalisé ;
si ce n'est pas le cas : vous avez 2 ans pour vous mettre en conformité.

2ans pour être en conformité
Si vous ne vous êtes pas mis en conformité d'ici la fin de ce délai, sachez néanmoins que la Cnil pourra à tout moment contrôler que le dispositif de biométrie mis en place dans votre entreprise répond aux obligations imposées par les nouvelles autorisations uniques.

Références :
(1) Article 25 de la Loi n°78-17 du 6 janvier 1978 modifiée, modifié par la Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
(2) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)
(3) Délibération n°2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique (AU-052)
(4) Délibération n°2016-187 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)…[Article source et complet]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et 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).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : Contrôles biométriques en entreprise : vos obligations changent !

Présidentielle 2017 : les candidats peuvent-ils exploiter vos données personnelles ?

Présidentielle 2017 : les candidats peuvent-ils exploiter vos données personnelles ?

+ DOCUMENT – Alors que les logiciels de stratégie électorale se généralisent et que l'organisation de primaires nécessite la mise en place de base de données, la CNIL rappelle dans un guide publié ce mardi les règles à respecter en matière de vie privée.…[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