

RGPD : Vol de données : la nouvelle norme



RGPD : Vol de données : la nouvelle norme

A six mois de l'entrée en vigueur du nouveau règlement européen sur la protection des données personnelles (RGPD) le 25 mai 2018 prochain, Proofpoint, spécialiste de la cybersécurité, dévoile les résultats de son étude paneuropéenne (Royaume-Uni, France, Allemagne) analysant le niveau de préparation des entreprises.

Les cyberattaques sont malheureusement devenues monnaie courante pour les entreprises qui doivent désormais intégrer pleinement les risques associés à leurs stratégies de sécurité pour se protéger. A l'image du piratage d'Equifax exposant les données personnelles de plus de 145 millions de citoyens américains ou du ransomware Wannacry ayant affecté plus de 200,000 ordinateurs dans 150 pays, tout le monde est concerné.

La France, semble particulièrement affectée, avec 61% des entreprises françaises qui déclarent avoir subi un vol de données personnelles durant les deux années écoulées (54% au Royaume Uni et 56% en Allemagne) et 78% d'entre elles qui redoutent un vol de données dans les 12 mois à venir (54% au Royaume-Uni et 46% en Allemagne).

Niveau de préparation RGPD : un décalage évident entre perception et réalité

Si les décideurs IT français semblent mieux préparés que leurs voisins (51% des répondants français pensent que leur organisation est déjà en conformité avec la réglementation RGPD, contre 45% au Royaume-Uni et 35% en Allemagne), l'étude révèle que plus d'une entreprise française sur cinq (22%) ne sera toujours pas en conformité avec la réglementation lors de son entrée en vigueur en mai 2018 (23% au Royaume-Uni et 34% en Allemagne). Un résultat finalement peu surprenant, considérant que seules 5% des entreprises auraient effectivement mis en place toutes les stratégies de gestion de données nécessaires pour garantir cette mise en conformité.

Les décideurs IT semblent pourtant conscients des enjeux, puisque 66% des répondants confient que leur budget a augmenté en prévision de l'entrée en vigueur de RGPD. Plus de sept entreprises sur dix en Europe ont par ailleurs monté des équipes projet dédiées RGPD et plus d'une sur quatre a désigné un responsable de la protection des données. A l'épreuve des faits, et alors que les entreprises avaient deux ans pour se préparer (adoption de la réglementation en avril 2016), seuls 40% des répondants révèlent que leur organisation a rempli un formulaire de mise en conformité RGPD...[lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
 - **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
 - **MISE EN CONFORMITÉ RGPD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : RGPD : 1 entreprise française sur 5 ne sera pas en conformité ! | UnderNews

Mise en garde des utilisateurs de Google Home et autres enceintes « intelligentes »

	<p>Mise en garde des utilisateurs de Google Home et autres enceintes « intelligentes »</p>
---	--

Sûreté vocalement, une enceinte connectée assiste l'utilisateur dans les tâches de son quotidien. Quels enjeux posent cette technologie au regard de la vie privée des utilisateurs ?

Qu'est-ce qu'une enceinte connectée dite intelligente ?

Une enceinte connectée « intelligente » est un dispositif équipé d'un haut-parleur et d'un micro qui intègre un assistant vocal. Grâce à cet équipement, l'enceinte est capable d'interagir avec l'utilisateur pour lui délivrer un service suite à une requête vocale. L'assistant est en mesure de répondre à une question, donner la météo, régler le chauffage, activer des lumières, réserver un VTC/Taxi, acheter des billets...

Le principe général de fonctionnement se caractérise par 4 grandes étapes :

Etape 1 – L'utilisateur « réveille » l'enceinte à l'aide d'une expression clé (« Hey Snips » / « Ok Google » / « Hey Alexa »).

Etape 2 – L'utilisateur énonce sa requête.

Etape 3 – La parole prononcée est automatiquement transcrite en texte puis interprétée afin qu'une réponse adaptée soit fournie.

Etape 4 – L'enceinte repasse en « veille»

Certaines de ces enceintes enregistrent localement les requêtes de l'utilisateur de manière à lui laisser la maîtrise de ses données (ex. une enceinte connectée avec l'assistant vocal de Snips). D'autres en revanche, envoient ces requêtes dans le cloud, autrement dit sur les serveurs de traitement de la société (ex. Amazon Echo, Google Home...). Dans les deux cas, l'appareil (ou ses serveurs) peut être amené à conserver :

- Un historique des requêtes transcrites afin de permettre à la personne de pouvoir les consulter et à l'éditeur d'adapter les fonctionnalités du service.
- Un historique des requêtes audio afin de permettre à la personne de les réécouter et à l'éditeur d'améliorer ses technologies de traitement de la parole.
 - Les métadonnées associées à la requête comme par exemple, la date, l'heure, le nom du compte.

[...]

Nos conseils

1. Encadrer les interactions de ses enfants avec ce type d'appareils (rester dans la pièce, éteindre le dispositif lorsqu'on n'est pas avec eux) ;
2. Couper le micro / éteindre l'appareil lorsque l'on ne s'en sert pas ou lorsqu'on ne souhaite pas pouvoir être écouté ;
3. Avertir des instructions de l'enregistrement potentiel des conversations (ou couper le micro lorsqu'il y a des invités) ;
4. Vérifier qu'il est bien réglé par défaut pour filtrer les informations à destination des enfants.
5. Connecter des services qui présentent réellement une utilité pour vous, tout en considérant les risques à partager des données intimes ou des fonctionnalités sensibles (ouverture porte, alarme...) ;
6. Être vigilant sur le fait que les propos tenus face à l'appareil peuvent enrichir votre profil publicitaire ;
7. Ne pas hésiter à contacter les services supports en cas de questions et, le cas échéant, la CNIL.
8. Se rendre régulièrement sur le tableau de bord pour supprimer l'historique des conversations/questions posées et personnaliser l'outil selon vos besoins. Par exemple, définir le moteur de recherche ou la source d'information utilisé par défaut par l'assistant. Lire la suite

LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX - MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / OPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVZ de l'évolution de vos traitements
 - FORMATIONS / SENSIBILISATION
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AI RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmes/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JURIDIQUES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'Information & Informatique Légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DQSTFP (Numéro formateur n°93 84 89841 84).

☐
☐
☐

Régissez à cet article

Source : *Enceintes intelligentes : des assistants vocaux connectés à votre vie privée | CNIL*

Jouets connectés : Dangers pour votre vie privée dit la CNIL



Jouets connectés : Dangers pour votre vie privée dit la CNIL

La Présidente de la CNIL met en demeure la société GENESIS INDUSTRIES LIMITED de procéder à la sécurisation de jouets connectés à destination d'enfants : la poupée « My Friend Cayla » et le robot « I-QUE ».

Le robot « I-QUE » et la poupée « My Friend Cayla » sont des jouets dits « connectés ». Ils répondent aux questions posées par les enfants sur divers sujets tels que des calculs mathématiques ou encore la météo. Les jouets sont équipés d'un microphone et d'un haut-parleur et sont associés à une application mobile téléchargeable sur téléphone mobile ou sur tablette. La réponse est extraite d'Internet par l'application et donnée à l'enfant par l'intermédiaire des jouets.

Alertée, en décembre 2016, par une association de consommateurs sur le défaut de sécurité des deux jouets, la Présidente de la CNIL a décidé de réaliser des contrôles en ligne en janvier et novembre 2017. Elle a par ailleurs adressé un questionnaire en mars 2017 à la société située à Hong-Kong.

Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom...) mais également des informations renseignées dans un formulaire de l'application « My Friend Cayla App ».

Plusieurs manquements à loi Informatique et Libertés ont été constatés dont notamment :

1.

Le non-respect de la vie privée des personnes en raison d'un défaut de sécurité

Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou « appairer ») un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier (par exemple, avec un code PIN ou un bouton sur le jouet).

La personne située à une telle distance est en mesure d'entendre et d'enregistrer les paroles échangées entre l'enfant et le jouet ou encore toute conversation se déroulant à proximité de celui-ci.

La délégation de la CNIL a également relevé qu'il était possible de communiquer avec l'enfant situé à proximité de l'objet par deux techniques :

- soit en diffusant via l'enceinte du jouet des sons ou des propos précédemment enregistrés grâce à la fonction dictaphone de certains téléphones ;
- soit en utilisant les jouets en tant que « kit main libre ». Il suffit alors d'appeler le téléphone connecté au jouet avec un autre téléphone pour parler avec l'enfant à proximité du jouet.

La Présidente a considéré que l'absence de sécurisation des jouets, permettant à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter, à l'insu des enfants et des propriétaires des jouets et d'avoir accès aux discussions échangées dans un cercle familial ou amical, méconnaît l'article 1^{er} de la loi Informatique et Libertés selon lequel l'informatique « ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

2.

Le défaut d'information des utilisateurs des jouets

Alors que des informations personnelles sont traitées par la société, les contrôleurs de la CNIL ont constaté que les utilisateurs des jouets ne sont pas informés des traitements de données mis en œuvre par la société...[lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDREFP (Numéro formateur n°93 84 03041 84).

✕

✕

Réagissez à cet article

Source : *Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité | CNIL*

Alerte à la fausse « Mise en conformité RGPD »

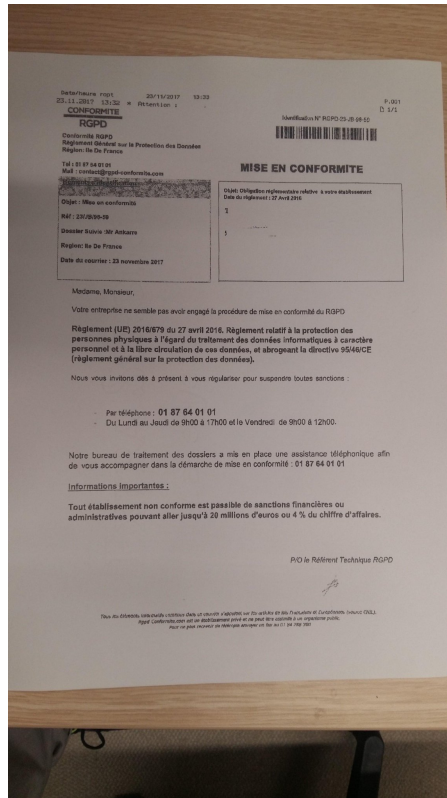
✖	Alerte à la fausse « Mise en conformité RGPD »
---	---

Des entreprises ont reçu par fax et par téléphone, en particulier ces derniers jours, des messages pour une « mise en conformité » avec le règlement européen sur la protection des données personnelles (dit « RGPD »). Le message, alarmiste et pouvant faire penser à une mise en demeure administrative, insiste sur les sanctions financières encourues.

Ces messages peuvent avoir pour but de vous faire appeler un numéro de téléphone surtaxé, de vous faire signer un engagement frauduleux pour une « mise en conformité Informatique et Libertés (ou RGPD) » ou de collecter des informations sur votre organisation pour préparer une escroquerie ou une attaque informatique.

La CNIL n'est, bien entendu, pas à l'origine de ces messages.

N'y répondez pas ! En cas de doute, vous pouvez contacter la vraie CNIL au 01 53 73 22 22.



Exemple de courrier RGPD frauduleux

- Ne répondez pas à cette sollicitation ;
- En cas de doute, contactez la CNIL au 01 53 73 22 22 ;
- Signalez cette arnaque au 0 811 02 02 17 ou sur le site www.internet-signalement.gouv.fr ;
- Consulter le site de l'agence nationale de sécurité des systèmes d'information (ANSSI) www.ssi.gouv.fr ;
- Consulter le site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques CERT-FR www.cert.ssi.gouv.fr ;
- Informez votre hiérarchie ;
- Déposez plainte si vous le souhaitez auprès des services de police ou de gendarmerie ou faite une déclaration directement sur le site de pré-plainte en ligne <https://www.pre-plainte-en-ligne.gouv.fr> ;
- Restez vigilant.

LE NET EXPERT

- MISE EN CONFORMITÉ RGPD / CNIL
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- MISE EN CONFORMITÉ RGPD de vos traitements
- SUIVI de l'évolution de vos traitements
- FORMATIONS / SENSIBILISATION :
- CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
- AU RGPD
- À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
- ORDINATEURS (Photos / E-mails / Fichiers)
- TÉLÉPHONES (récupération de Photos / SMS)
- SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- SÉCURITÉ INFORMATIQUE
- SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Ce qu'il faut savoir sur les jouets connectés

✕	Ce qu'il faut savoir sur les jouets connectés
---	---

S'ils s'invitent en nombre dans les magasins et sur les listes au Père Noël, les jouets connectés suscitent quelques craintes. Voici un petit guide pour s'y retrouver.

Tablettes, robots, peluches, jeux de société... Difficile de ne pas trouver une catégorie de jouets dont un ou plusieurs modèles n'aient pas une version connectée. De récents scandales montrent que le secteur n'est pas encore tout à fait au point pour que les plus jeunes puissent s'amuser en toute sécurité. En sept questions, Pixels fait le tour de cette tendance et des précautions à prendre pour que Noël ne tourne pas à une mise sur écoute.

[...]

Si l'on considère les jouets connectés au regard de la loi informatique et libertés, plusieurs questions s'avèrent importantes :

- le fabricant informe-t-il de façon claire les utilisateurs (en tout cas les parents) sur le fait que le jouet enregistre des données ? Recueille-t-il clairement leur consentement ? Le jouet ou l'appli invitent-ils bien les parents à réaliser cette étape importante au lieu de laisser l'enfant passer rapidement dessus ?
- est-il pertinent et nécessaire pour le fabricant de récupérer ces données ? Par exemple, est-il utile de demander l'adresse postale ou le nom complet d'un enfant pour faire fonctionner un jouet ? A quoi peuvent servir ces données au fabricant ?
- s'agissant de la sécurité de ces données : un mot de passe fort est-il requis ? Comment les données sont-elles chiffrées, où sont-elles stockées, et pendant combien de temps ? Qui peut y accéder ?

Les fabricants font-ils attention ?

Difficile de répondre puisque les fabricants ne sont mis en défaut que lorsqu'un problème de protection des données ou de vulnérabilité du jouet surgit, souvent bien après la commercialisation du produit.

En ce qui concerne la France, certains fabricants consultent en amont la Commission nationale informatique et libertés (CNIL) pour s'assurer d'être en conformité avec la loi. D'autres sont moins scrupuleux par souci d'économies. Ils utilisent par exemple des composants standards, parfois peu sécurisés, pour que le jouet ne soit pas trop cher.

Il y a aussi une limite technique. Si, après la mise sur le marché, un fabricant souhaite apporter une correction, il peut le faire sur une application ou un logiciel mais pas sur le jouet lui-même. Il faudrait rappeler le produit...[lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
 - **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
 - **MISE EN CONFORMITÉ RGPD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

70 % des attaques informatiques partent d'un problème humain. Il est urgent de sensibiliser votre personnel.

	<p>70 % des attaques informatiques partent d'un problème humain. Il est urgent de sensibiliser votre personnel.</p>
--	--

En matière de cybersécurité, l'Europe a décidé de légiférer mais des disparités existent. Explications avec Julie Gommès, experte en cybersécurité lors de la SME Assembly 2017 (Assemblée annuelle des PME organisée par la Commission européenne) à Tallinn (Estonie). Pour elle, la première faille de sécurité est entre la chaise et l'ordinateur.

[Article source]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
 - **ÉTAT DES LIEUX RGPD** de vos traitements)
 - **MISE EN CONFORMITÉ RGPD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
 - **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *Cybersécurité : 70 % des attaques partent d'un problème humain – Courrier cadres*

Plusieurs centaines de sites enregistrent l'intégralité des actions de visiteurs

✕	Plusieurs centaines de sites enregistrent l'intégralité des actions de visiteurs
---	---

Une étude menée par des chercheurs de l'université de Princeton montre que des sites très populaires recourent à des scripts qui enregistrent le moindre mouvement de souris.

La pratique s'appelle session replay, littéralement « rejouer une session ». Elle consiste à enregistrer l'intégralité des actions d'un visiteur sur un site Web : les endroits où il clique bien sûr, mais aussi ses mouvements de souris, ce qu'il ou elle tape dans un formulaire de série et à quelle vitesse... Des données qui permettent de « revoir », en vidéo, comment un internaute s'est comporté en reproduisant l'intégralité de sa session sur le site...[lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *Plusieurs centaines de sites enregistrent l'intégralité des actions de visiteurs*

Vol de données chez Uber : L'état Français demande des explications

✕	Vol de données chez Uber : L'état Français demande des explications
---	---

Le secrétaire d'État au Numérique a écrit jeudi au PDG d'Uber, Dara Khosrowshahi, après l'annonce du piratage des données personnelles de 57 millions d'utilisateurs.

Le secrétaire d'État au Numérique Mounir Mahjoubi a écrit jeudi au PDG d'Uber, Dara Khosrowshahi, après l'annonce du piratage des données personnelles de 57 millions d'utilisateurs, pour lui demander des explications sur d'éventuelles victimes françaises.

« Face au danger que représente l'exploitation de ces données, je souhaite vous exprimer mon inquiétude quant à l'éventuelle présence en très grand nombre de clients et chauffeurs français » parmi les victimes, souligne Mounir Mahjoubi, dans un courrier. « Pouvez-vous à ce jour nous indiquer si des utilisateurs français sont concernés et si oui combien, et de quel type sont les données qui ont été dérobées », interroge-t-il. Le secrétaire d'État demande aussi « quelles mesures techniques et organisationnelles sont mises en place pour informer et accompagner les utilisateurs ».

Noms, adresses électroniques et numéros de téléphone.

Uber n'a pas détaillé qui sont les victimes de cette fuite d'informations remontant à la fin 2016, et qu'il avait dissimulée, mais de nombreux Français sont vraisemblablement concernés. Le chiffre de 57 millions est en effet énorme, quand l'ancien patron Travis Kalanick déclarait en octobre 2016 -plus ou moins au moment des faits- compter 40 millions d'utilisateurs actifs dans le monde. Selon Uber, les noms, adresses électroniques et numéros de téléphone des victimes ont été subtilisés. Le groupe américain de réservation de voitures avec chauffeur affirme qu'aucune information bancaire n'a été exfiltrée, pas plus que les dates de naissance et les historiques de trajets.

Le secrétaire d'État s'étonne qu'Uber n'ait « pas signalé cet incident ». Mounir Mahjoubi s'étonne également de ce qu'Uber n'ait « pas signalé cet incident » auprès de la Commission nationale de l'informatique et des libertés (Cnil) et de l'Agence nationale de la sécurité des systèmes d'information (Anssi), responsables respectivement de la protection des citoyens et de la coordination de la défense française contre les pirates informatiques, qui ont été mises en copie de son courrier. Il aurait également apprécié que le groupe américain se signale « auprès des utilisateurs concernés ».

Mahjoubi souhaite que l'entreprise informe les utilisateurs concernés et les autorités. « Au regard du nombre de vos clients, vous avez une importance qui vous donne des responsabilités », souligne Mounir Mahjoubi, rappelant qu'un règlement européen rendra en mai prochain les entreprises responsables des données personnelles qu'elles détiennent, et leur imposera de signaler rapidement les incidents. « Au regard du danger existant, nous aimerions que vous informiez volontairement les utilisateurs concernés ainsi que les autorités françaises », insiste le secrétaire d'État au Numérique...[lire la suite]

LE NET EXPERT

:

- MISE EN CONFORMITÉ RGPD / CNIL
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- MISE EN CONFORMITÉ RGPD de vos traitements
- SUIVI de l'évolution de vos traitements
- FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *Piratage d'Uber : Mahjoubi demande des explications*

Uber : ces inquiétants témoignages de Français qui rapportent des piratages



Uber : ces inquiétants témoignages de Français qui rapportent des piratages

La révélation fin novembre 2017 du hacking géant de Uber, qui s'est fait voler les données de 57 millions d'utilisateurs à travers le monde, a de quoi inquiéter les habitués de l'appli. Si l'entreprise assure que leurs coordonnées bancaires sont à l'abri, des Français témoignent avoir vu leur compte piraté pour des sommes parfois très conséquentes.

Un séisme dans le joyeux monde des applis. La direction d'Uber a admis cette semaine que les données de 57 millions de ses utilisateurs avaient été piratées en octobre 2016. Après avoir donc dissimulé ce hacking d'ampleur pendant un an, l'entreprise s'est empressée d'assurer ce mardi 21 novembre que les coordonnées bancaires des usagers concernés n'avaient pas été dérobées. « *Cela me paraît très bizarre qu'Uber ne stocke qu'une partie des données dans son Cloud Amazon, celui qui a été hacké par les pirates, sans les numéros de cartes bancaires* », relève pour Marianne Julie Gommès, experte en cyber-sécurité. « *Que les données bancaires ne soient pas du tout concernées me semble peu probable* », abonde Claire Juiff, experte conseil en gestion de crise et formée au cyber-risque...[lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGD / CNIL**
- **AUDIT RGD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *Uber : ces inquiétants témoignages de Français qui rapportent des piratages*

**RGPD : les petites
entreprises tout aussi
concernées que les grandes**

✕	RGPD : les petites entreprises tout aussi concernées que les grandes
---	---

Le règlement général européen sur la protection des données sera mis en œuvre le 25 mai 2018 pour améliorer la protection et la confidentialité des données et responsabiliser davantage les entreprises en développant l'auto-contrôle. Celles-ci devront dorénavant s'assurer que toutes les données qu'elles stockent sont en conformité avec la réglementation.

Le 25 mai prochain, toutes les entreprises devront se conformer à la nouvelle réglementation générale des données personnelles (RGPD). Celle-ci vise à établir des règles claires et unifiées pour que les individus puissent mieux contrôler les données qui les concernent. Les obligations visent toutes les entreprises, en B to B comme en B to C, quelle que soit leur taille, à partir du moment où elles collectent, traitent, gèrent et utilisent des données, que ce soit des fichiers collaborateurs en interne ou des données sur leurs clients ou fournisseurs. « Un ancien candidat qui a envoyé son CV à l'entreprise pour y postuler constitue par exemple une donnée collectée » cite Nathalie Rouvet Lazare, PDG de Coheris qui édite des solutions CRM et analytiques sur le sujet.

Toutes les données stockées sont concernées

Les données considérées comme personnelles sont nombreuses : nom, adresse, localisation, identifiant, date de naissance, IP..., autrement dit toutes les données qui permettent d'identifier une personne. Même si les données ne sont pas utilisées et traitées, à partir du moment où elles sont stockées au sein de l'entreprise, elles sont concernées par la réglementation. Même chose en termes de forme : tous les fichiers, du tableur Excel aux bases de données de prospects, salariés ou visiteurs d'un site Internet ou d'une boutique physique, sont visés. Nathalie Rouvet Lazare se veut rassurante : « Les petites entreprises doivent elles aussi se mettre en ordre de marche et établir une feuille de route. Il ne faut pas y voir une usine à gaz ou une contrainte de plus mais utiliser cette nouvelle réglementation comme une opportunité pour optimiser les données de l'entreprise ». Si celles-ci ont tendance à collecter un maximum de données, au final, peu d'entre elles les utilisent. « Elles devront dorénavant mener une réflexion préalable sur leur objectif pour chaque donnée collectée. »

Se conformer au règlement en 3 étapes

Pour mettre en place une gouvernance des données personnelles, les entreprises doivent commencer par :

- nommer une personne référente au sein de l'entreprise qui sera le pilote responsable de la mise en place des process et des outils. « Si les entreprises n'ont pas l'obligation légale de nommer un DPO (Data Protection Officer ou Délégué à la Protection des Données), il est essentiel de désigner un porteur de projet sur le sujet. »

- réaliser un audit, soit cartographier toutes les données personnelles et sensibles de l'entreprise, définir dans quels types de fichiers elles sont utilisées et comment elles sont gérées.

- passer au crible ses obligations et définir ses process et responsabilités pour s'assurer qu'elle est en conformité avec la loi.

L'occasion de mettre en place plusieurs bonnes pratiques pour répondre aux nouvelles obligations liées à la RGPD, comme un process pour protéger les données dès leur conception – data protection de by design–, la vérification de la protection effective de ses données, l'élimination des données récoltées de façon illicite ou déloyale, la révision de ses procédures de consentement qui doit être clair et circonstancié. Et si l'entreprise souhaite partager ses données personnelles avec ses partenaires, elle doit en préciser l'identité et la finalité du partage. C'est ce que l'on appelle la récolte opt-in. Enfin, avec la RGPD, les entreprises doivent être en mesure de respecter l'exercice du droit d'opposition, de rectification, d'accès direct, de portabilité et d'effacement des données...[lire la suite]

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD** ? ?

Besoin d'une **formation pour apprendre à vous**

mettre en conformité avec le RGPD ?

Contactez-nous

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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 étapes

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 : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles



Réagissez à cet article

Source : Protection des données : les petites entreprises tout aussi concernées que les grandes