

Vos enfants à l'École : Quelle protection des données personnelles ?



Vos enfants
à l'École :
Quelle
protection
des données
personnelles ?

Jamais la question de la vie privée n'aura été autant abordée ces dernières années. De nombreuses solutions fleurissent pour protéger ses données personnelles au quotidien mais au sein de l'école, avec le numérique, les actions sont encore floues.

Pourquoi c'est dangereux ?

Cette entrée dans la vie privée des élèves est grave, comme l'explique à La Croix Gilles Dowek, président du conseil scientifique de la Société informatique de France : « **ces données pédagogiques sont bien plus sensibles que les données médicales**, car elles concernent des enfants, qui construisent leur personnalité, et il serait grave de leur assigner des erreurs qui les suivront le reste de leurs vies ». En clair, les bulletins de notes ou autres appréciations des professeurs font partie des informations qui peuvent être récupérées par les GAFAM et ainsi poursuivre les enfants tout au long de leur vie scolaire, universitaire et professionnelle...[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 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 : <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.

Source : École : quelle protection des données personnelles de vos enfants ?

Comment faire disparaître ses données d'Internet ?



Il est aujourd’hui difficile de limiter l’utilisation de nos données personnelles par les entreprises, mais une loi pourrait bientôt nous faciliter la tâche.

Un procédé complexe

Non, il n’existe pas de formulaire « plainte » ou « comment disparaître de nos bases de données » sur les sites qui utilisent nos données. Selon Daniela Parrot, responsable du service plaintes de la CNIL (la Commission nationale pour l’informatique et les libertés), il faut en premier lieu « identifier l’entreprise » qui possède les données qui vous posent problème. Pour cela, vérifier les mentions légales de leur site internet permet de savoir quelles données l’entreprise se permet d’utiliser à des fins commerciales. Il convient ensuite d’écrire un courrier à l’entreprise, d’évoquer un motif (commercial ou autre) et de pouvoir apporter une preuve (un scan par exemple) de ce courrier pour pouvoir déposer une plainte à la CNIL en cas d’absence de réponse. Il faut aussi ne pas oublier de joindre sa pièce d’identité.

Les entreprises bientôt limitées ?

Pour une meilleure harmonisation de la protection des données dans l’UE, le *Règlement général sur la protection des données* (le « GDPR ») sera applicable en mai 2018, après quatre années de négociations législatives au sein du parlement européen. Bien que la plupart des entreprises ont entamé des processus de régularisation, de nouvelles limitations vont les forcer à revoir leur politique. Seulement 10% des boîtes implantées dans l’Union Européenne seraient en mesure de faire face à ces mesures...[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
- MISE EN CONFORMITE RGPD / FORMATION DPO

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 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 : <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 DTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Source : *Comment faire disparaître ses données d'Internet ?*

RGPD : une nécessité, de nouvelles exigences !



Le Règlement général sur la protection des données entre en vigueur en 2018 et prévoit la mise en pratique de nouvelles exigences pour les entreprises.

Pour renforcer la protection des données personnelles, le nouveau Règlement général sur la protection des données (RGPD) s'attache à défendre les droits des consommateurs et à établir de nouvelles normes pour la sécurité des entreprises. Il est crucial que celles-ci procèdent, de la même façon avec les données numériques qu'avec des documents confidentiels conservés dans un coffre-fort. A défaut de mesures de protection efficaces, ces données peuvent être copiées illégalement et, dans les cas les plus graves, diffusées ou revendues. On ne parle plus uniquement de protection des données, mais de trésor des données : les protéger signifie également protéger l'entreprise.

Une architecture conforme au RGPD

Chaque réglementation inclut des contraintes pour les entreprises. Concernant la RGPD, les 4 principales sont les suivantes :

- Garantir la sécurité et l'intégrité des données : les fichiers qui contiennent des données personnelles ne doivent être accessibles qu'à des personnes autorisées. Les répertoires doivent être soumis à un contrôle permanent devant permettre de tracer les copies et les modifications. En cas d'incident relatif à la sécurité, les différents départements et le service informatique doivent être en position de fournir des informations et des explications sur l'incident.
- La documentation des droits d'accès : la notion de responsabilité exige que les institutions traitant des données soient à tout moment en mesure de démontrer qu'elles disposent de l'historique des droits d'accès ainsi que des accès effectués par le passé.
- Mise à jour des permissions : particulièrement dans le cas des personnes qui arrivent dans une entreprise, changent de poste ou la quittent, le service informatique et les départements concernés sont tenus de disposer d'une vue d'ensemble des permissions détenues par les employés et de pouvoir les modifier rapidement, sachant que le vol de données s'effectue le plus souvent lors du départ d'un employé. Le département concerné doit avoir annulé les droits d'accès aux répertoires importants pour la sécurité de tout employé quittant l'entreprise avant son départ.
- La création d'un « responsable de données » : cette nouvelle réglementation exige une répartition claire des responsabilités pour le traitement des données personnelles. Dans cette optique, la création du rôle de « Responsable de données », est d'une importance cruciale. Les responsables de données sont des cadres chargés au sein de leur département de surveiller le traitement des données. Ils doivent savoir quels sont les répertoires qui nécessitent une protection et quels sont les employés auxquels ils peuvent accorder leur confiance. La création de nouvelles fonctions telles que celle-ci exige simultanément la mise en place de nouveaux processus de collaboration de la documentation des activités mises en œuvre...[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 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 : <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 DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Editeurs de logiciels: pourquoi vos clients vont vous contraindre à justifier de la conformité au RGPD de vos outils ?



Editeurs de logiciels:
pourquoi vos clients vont vous contraindre à justifier de la conformité au RGPD de vos outils ?

Les éditeurs de logiciels devront dorénavant faire la démonstration de la conformité de leurs solutions au Règlement général de protection des données, lequel entrera en vigueur le 25 mai 2018.
La Cnil a eu l'occasion de l'affirmer à plusieurs reprises, et le règlement européen en matière de protection des données (RGPD) ne change rien à la situation sur ce point: les éditeurs de logiciels ne sont pas considérés comme responsables de traitement. Seuls les clients utilisateurs le sont par principe. Mais alors, pourquoi les éditeurs font-ils face à des demandes urgentes de leurs clients, les pressant de fournir des preuves de la conformité de leurs produits au RGPD? Le règlement européen modifie le management de la conformité en imposant l'accountabilité. Les responsables de traitement doivent donc, dorénavant, démontrer leur conformité. L'accountabilité implique pour les responsables de traitement de déterminer des mesures techniques et organisationnelles permettant de démontrer que les traitements qu'ils mettent en oeuvre sont conformes au RGPD.

L'importance du programme de management de la conformité

L'accountabilité nécessite de déterminer un programme de management de la conformité en matière de protection des données. Ce programme doit contenir notamment une procédure de violation des données, des politiques de sécurité et de durée de conservation mais également des procédures permettant de s'assurer que les principes de protection par défaut et dès la conception sont appliqués. Si la protection dès la conception pour un responsable de traitement lui impose de déterminer les règles et fonctions nécessaires à la protection des données pour les outils qu'il crée ou développe en interne, il doit également vérifier, lorsqu'il acquiert des droits d'utilisation d'un outil édité par un tiers, que cet outil intègre l'ensemble des fonctions, paramétrages et spécifications requis pour respecter les obligations du RGPD. Cela signifie, pour les outils qu'ils prennent sous licence, que les responsables de traitement doivent exiger de leurs éditeurs qu'ils attestent de la conformité de leurs produits. Ainsi, les responsables de traitements sont à même de démontrer qu'ils respectent leurs propres obligations...[lire la suite]

Commentaire de Denis JACOPINI

Depuis plusieurs années, les éditeurs de logiciels auraient dû assurer l'évolution de leurs logiciels par rapport à la réglementation en général et la protection des données personnelles en particulier.

En effet, depuis plus de 30 ans, les données inutilisées doivent faire l'objet d'une anonymisation ou d'une suppression. Quel éditeur de logiciel dispose de cette fonction de suppression ou d'anonymisation par rapport à une date de dernière utilisation? Non seulement quasiment aucun, mais ceux à qui leurs clients leur demandent de respecter la réglementation en général envoient en retour pour les plus audacieux un insolent devis, et une réponse négative pour les plus téméraires. Heureusement que l'évolution de la réglementation au travers du RGPD va faire évoluer les choses par la force, car ce n'est pas au client final ni de payer les évolutions réglementaires des logiciels ni la résolution des dysfonctionnements en cachant l'amélioration de leurs failles dans des mises à jour payantes.

Accepteriez-vous que votre garage vous fasse payer la réparation des défauts de fabrication de votre voiture?

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 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 : <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 ».
• Audit Sécurité (ISO 27005);
• Expertise technique et judiciaire (Avis techniques, expertises de preuves téléphones, disques durs, e-mails, conteneurs, débrouillages de clientèle...);
• Expertises sur systèmes de vote électronique ;
• Formations et conférences en cybercriminalité ;
• Autorisation de la CIL (n°93 84 03041 84);
• Formation de C.I.L (Correspondants Informatique et Libertés);
• Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : [Tribune] Editeurs de logiciels: pourquoi vos clients vont vous contraindre à justifier de la conformité au RGPD de vos outils?

RGPD 2018 : Quels impacts sur vos actions marketing ?

email
stratégie

WEBINAIRE
PRÉPAREZ-VOUS !

Quels impacts pour vos
actions marketing ?

RGPD 2018



**RGPD 2018 :
Quels impacts
sur vos
actions
marketing ?**

Le RGPD c'est bientôt ! Si vous ne savez pas ce qui se trame derrière ces 4 lettres, il est impératif que vous consaciez une partie de votre temps à son sujet. L'échéance pour être en conformité avec le nouveau règlement Européen est fixée au 25 mai 2018, autant dire demain pour les entreprises.

Le Règlement Général de la Protection des Données (aka RGPD ou GDPR) c'est certainement le dossier le plus épique de 2018. Véritable défi d'envergure mondiale pour les professionnels du marketing et de la data. Les structures qui seront capables de négocier ce virage imposé, auront un véritable avantage concurrentiel. Car les sanctions prévues en cas de manquement aux règles sont colossales tant en termes de déficit d'image qu'en termes financiers. D'ailleurs, les sanctions auront de quoi décourager les entreprises les plus téméraires, car un seul contrôle des autorités sera quasiment synonyme de fermeture pour une large majorité d'entre elles...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre

expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles> (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)



Réagissez à cet article

Source : *RGPD 2018 : Quels impacts sur vos actions marketing ? – Métier*

Les collectivités face à la protection des données personnelles



Certaines de nos données personnelles peuvent figurer un peu partout : dans des documents administratifs, dans des fichiers, sur Internet... Deux lois de 1978 régissent les cas de communication et de traitements automatisés. Des directives européennes sont venues réglementer l'open data mais les demandes de suppression de données privées sur les moteurs de recherche ne sont pas encore suivies d'effet. La jurisprudence est en cours de réflexion sur ce point.

La loi 78-17 du 6 janvier 1978 dite Informatique et libertés (ici en version actualisée) protège les droits des personnes dans le cadre des traitements automatisés et des fichiers. Elle fut suivie de la loi 78-753 du 17 juillet 1978 qui concerne la liberté d'accès aux documents administratifs. Il est très important de ne pas confondre les deux lois qui n'ont pas les mêmes objets. Le respect de l'application de la première de ces deux lois relève de la CNIL (commission nationale informatique et libertés) alors que le respect de la seconde loi de 1978 relève de la Cada (commission d'accès aux documents administratifs). De plus, un code spécial a été créé pour regrouper toutes les dispositions relatives à la seconde loi et à la Cada : le CRPA (code des relations entre le public et l'administration) créé par une ordonnance du 17 mars 2016.

Enfin, il existe dans toutes les collectivités un référent CNIL dont la fonction, actuellement facultative, deviendra obligatoire dès mai 2018 pour l'ensemble des organismes du secteur public. Et, depuis 2005, un référent Cada (désigné sous l'appellation de « Prada » : personne responsable de l'accès aux documents administratifs et des questions relatives à la réutilisation des informations publiques)...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)



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.



Contactez-nous



Réagissez à cet article

Source : *La protection des données personnelles – AgoraVox le média citoyen*

RGPD : La Cnil invite les collectivités à se mettre à la page



**RGPD : La
Cnil invite les
collectivités à se mettre à
la page**

Alors que l'application du Règlement général sur la protection des données deviendra obligatoire le 25 mai 2018. La Cnil souligne le manque de préparation d'un grand nombre de collectivités territoriales.

La Cnil s'appuie sur une enquête de la Gazette des communes, qui affirme que seules 10% des collectivités se sentent prêtes pour leur mise en conformité d'ici à mai 2018.

Au vu du grand nombre de données personnelles générées par les collectivités territoriales, notamment grâce au développement de l'e-administration les obligeant à recourir de plus en plus aux technologies numériques telles que les téléservices par exemple. Leur mise en conformité devient nécessaire.

Aider les collectivités à mieux se préparer

La Cnil apporte donc quelques préconisations aux collectivités pour qu'elles atteignent dans les délais leur mise en conformité.

La commission insiste sur le fait "qu'elles [collectivités] devront adopter et actualiser des mesures techniques et organisationnelles leur permettant de s'assurer et de démontrer à tout instant qu'elles offrent un niveau optimal de protection aux données traitées."

Qui plus est, la désignation d'un correspondant informatique et libertés (CIL) qui endossera le rôle de délégué à la protection des données est requise.

Jusqu'à présent la nomination d'un CIL était facultative, elle devient obligatoire en mai 2018, pour que le délégué puisse s'assurer de la "mise en oeuvre de la conformité au règlement européen dans son organisme", précise la Cnil...[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 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)

de la formation professionnelle n° 93-34-03041-34, d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

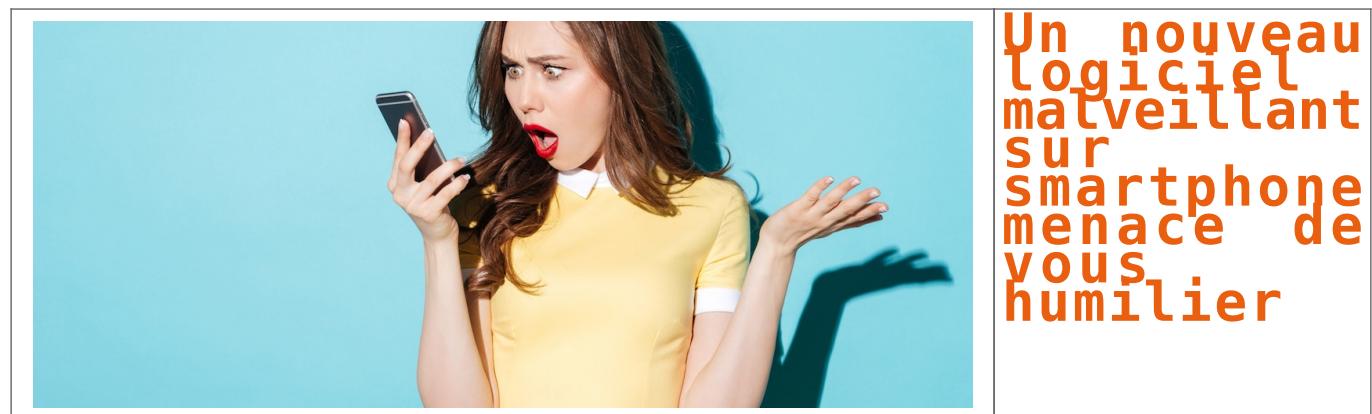


Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- 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 DRTF n°93 84 (3041 84))
 - Formation de C.I.L. (Correspondants Informatique et Libertés) ;
 - Accompagnement à la mise en conformité CNIL de votre établissement.

Source : RGPD : La Cnil invite les collectivités à se mettre à la page | Archimag

Un nouveau logiciel malveillant sur smartphone menace de vous humilier



Un nouveau logiciel malveillant sur smartphone menace de vous humilier

Un logiciel de rançon nommé «LeakerLocker» menace d'envoyer vos courriels, messages texte, photos et votre historique web à tous vos contacts si vous ne versez pas une somme de 50\$ à ceux qui prennent en otage vos informations personnelles.

Découvert la semaine dernière par l'éditeur d'antivirus McAfee, LeakerLocker vise exclusivement les utilisateurs de téléphones Android. Au moins deux applications gratuites qui ont désormais été retirées de la plateforme Google Play, «Wallpapers Blur HD» et «Booster & Cleaner Pro», ont été identifiées comme les entremetteuses du ransomware.

«Les deux [applications] offrent des fonctionnalités qui semblent normales, mais cachent une charge utile malicieuse», explique McAfee dans un billet publié sur son blogue.

Payer ou non?

Une fois qu'un téléphone est infecté par LeakerLocker, son écran d'accueil se verrouille et explique à la victime que toutes ses informations personnelles ont été sauvegardées dans le Cloud. «Ces données seront envoyées à [...] votre liste de contacts dans moins de 72 heures. Pour annuler cette action, vous devez payer une modeste RANSOM [sic] de 50\$, poursuit le message.



CAPTURE D'ÉCRAN – MCAFEE

Ce que les victimes de LeakerLocker voient sur leur écran de téléphone cellulaire.

McAfee indique pourtant que le logiciel n'a pas accès à autant d'informations qu'il ne laisse présager. Bien qu'il soit entièrement capable de consulter l'historique de navigation et l'adresse courriel de la victime, l'accès aux contacts, aux messages texte et aux photos n'est que partiel. Considérant ces faits, il est impossible de déterminer si les menaces sont légitimes ou si toute cette histoire s'agit simplement d'une arnaque. L'éditeur de logiciels antivirus avise le public de ne pas dépenser d'argent dans une telle situation puisque plier à des demandes de ranonneurs web «contribue à la prolifération de cette industrie malveillante».

Source : *Un nouveau logiciel malveillant menace de vous humilier à l'aide de vos données personnelles | JDM*

Notre métier : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec le RGPD (règlement Européen relatif 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, Recherches de preuves téléphones, disques durs, e-mails, conteneurs, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Un nouveau logiciel malveillant menace de vous humilier à l'aide de vos données personnelles | JDM*

Règlement européen sur la protection des données (RGPD) : votre collectivité sera-t-elle prête pour 2018 ?



Règlement européen sur la protection des données (RGPD) : votre collectivité sera-t-elle prête pour 2018 ?

Parce que votre opinion nous intéresse, La Gazette a constitué un panel de fonctionnaires territoriaux que nous interrogeons sur l'actualité des politiques publiques et du statut de la fonction publique. Cette semaine : votre collectivité sera-t-elle prête en 2018 pour mettre en œuvre le règlement européen sur la protection des données ?

Les craintes se confirment : **seuls 10 % des territoriaux pensent que leur collectivité sera prête le 25 mai** pour l'entrée en vigueur du règlement général de l'Union européenne sur la protection des données, adopté le 27 avril 2016. Un faible pourcentage qui fait écho au constat établi le 27 mars par Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés : « Moins de 10 % des entreprises estiment qu'elles seront prêtes à temps. » Pourtant, les collectivités n'ont pas le choix puisqu'elles devront absolument appliquer ce texte à compter du 25 mai. L'une des principales obligations qui en découle est la mise en place d'un délégué à la protection des données, sorte de successeur du correspondant informatique et libertés, et qui sera pilote de la conformité...[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 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 : <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.

Source : *Règlement européen sur la protection des données : votre collectivité sera-t-elle prête pour 2018 ?*

Marre du spam ? Votre signalement enfin utile !



**Marre du spam ?
Votre signalement
enfin utile !**

La Cnil annonce s'être rapprochée de l'association Signal Spam pour mieux agir contre les courriers indésirables. L'organisation en profite pour annoncer un changement de tactique et pour indiquer l'existence d'un outil permettant de signaler le spam très facilement.

« le contenu de ces mails seront transmis au service de l'association Signal Spam pour analyse. votre signalement permet d'identifier les criminels, d'informer les autorités, d'être automatiquement désinscrit auprès des routeurs membres, d'imposer des pratiques commerciale plus respectueuses des internautes et bien sûr d'améliorer la protection de votre ordinateur »

Votre boîte aux lettres reçoit un peu trop de courriers indésirables à votre goût ? Vous avez beau prendre garde à ne pas laisser traîner votre adresse électronique n'importe où, vous avez chaque jour du spam qui se mêle à votre correspondance ? Les filtres des grandes messageries, comme Gmail, ne vous donnent pas entière satisfaction ? Alors peut-être est-il temps d'envisager une autre approche.

Vous avez la possibilité de vous inscrire sur le site de l'association Signal Spam et de télécharger une extension pour navigateur (elle est disponible pour Firefox, Chrome et Safari) ou un module pour votre logiciel de messagerie (Thunderbird, Outlook, Mail OSX Sierra, Mail OSX El Capitan). Une fois cela fait, vous pourrez signaler des spams en un seul clic.

Une vidéo de mise en route est fournie par la Commission nationale de l'informatique et des libertés (Cnil).

Dans les grandes lignes, une fois que vous avez téléchargé le module et l'avez configuré, il vous suffit d'ouvrir le spam que vous avez reçu dans votre boîte aux lettres et de cliquer sur l'icône de signalement. Le logiciel récupérera alors le contenu du courrier indésirable...[lire la suite]

Notre métier : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec le RGPD (règlement Européen relatif 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.



Réagissez à cet article

Source : Marre du spam ? La Cnil vous invite à envoyer des signalements en un clic via le navigateur – Tech – Numerama