

Il diffusait des dizaines de données personnelles piratées sur Internet

✕	Il diffusait des dizaines de données personnelles piratées sur Internet
---	---

L'information provient de la plateforme Pharos qui permet à tout le monde de signaler un contenu suspect ou illicite sur Internet.

En février 2014, les forces de police s'intéressent donc à un site qui diffuse des dizaines de données personnelles piratées dont des numéros de carte bancaire et des scans de carte d'identité. La brigade de lutte contre la cybercriminalité de Lens est saisie. Les policiers remontent jusqu'à un habitant de Nœux-les-Mines. Convoqué au commissariat, il reconnaît avoir un certain attrait pour la sécurité des réseaux Internet.

Suite à une perquisition, son ordinateur est saisi. Et là, les découvertes s'enchaînent. En plus des données personnelles piratées, les enquêteurs retrouvent également plusieurs logiciels de piratage qui permettent de prendre le contrôle sur des sites mais aussi sur des ordinateurs à distance et, enfin, de modifier le contenu de bases de données.

Une cinquantaine de victimes

Autant de faits qui constituent des délits. Le mis en cause, 25 ans, est aujourd'hui poursuivi pour six d'entre eux.

Si le dossier a mis autant de temps à être bouclé c'est aussi qu'il fallait retrouver l'ensemble des victimes. Et elles sont nombreuses. Une cinquantaine a été retrouvée à ce jour, dont l'entreprise d'informatique Microsoft.

Autant de personnes face auxquelles le prévenu devra s'expliquer lors de l'audience correctionnelle prévue le 5 septembre.

NOTRE MÉTIER :

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

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister 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 : *Il diffusait des dizaines de données personnelles piratées sur Internet – La Voix du Nord*

Un nouveau logiciel malveillant sur smartphone menace de vous humilier



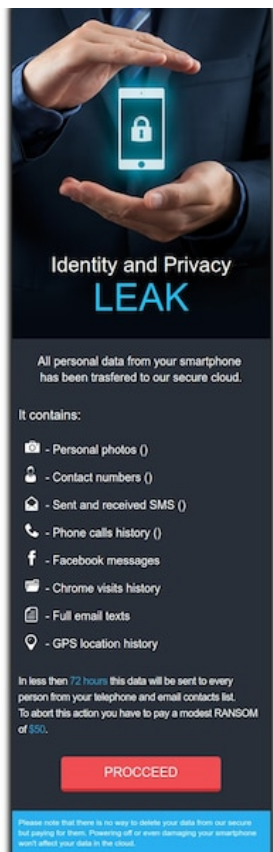
Un logiciel de rançon nommé «LeakerLocker» menace d'envoyer vos courriels, messages texte, photos et votre historique web à tous vos contacts si vous ne versez pas une somme de 50\$ à ceux qui prennent en otage vos informations personnelles.

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 rançonneurs 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>



Réagissez à cet article

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>



Réagissez à cet article

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>



Réagissez à cet article

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

Peut-on accéder aux données personnelles d'une personne décédée ?



Peut-on
accéder aux
données
personnelles
d'une
personne
décédée ?

Le fils d'une personne décédée ne peut pas avoir accès aux données de cette dernière car il n'est pas considéré par la loi de 1978 comme la personne concernée.

Toutefois, indique le Conseil d'Etat dans sa décision du 7 juin 2017, sera considérée comme personne concernée, l'ayant droit d'une personne décédée qui avait été victime d'un dommage, et dont le droit à réparation de ce dommage, entré dans son patrimoine, est ainsi transféré à ses héritiers.

Un fils avait adressé une plainte à la Cnil car il estimait que la mutuelle de sa mère n'avait pas répondu à sa demande d'accès aux données de cette dernière. La mère en question avait été victime d'un accident de circulation et une procédure judiciaire avait été engagée afin de déterminer la réparation du préjudice subi. La Cnil avait clôturé sa plainte au motif que le droit d'accès conféré aux personnes physiques par l'article 39 de la loi Informatique et libertés est un droit personnel qui ne se transmet pas aux héritiers. Le Conseil d'Etat a annulé la décision de la présidente de la Cnil car « *lorsque la victime a engagé une action en réparation avant son décès ou lorsque ses héritiers ont ultérieurement eux-mêmes engagé une telle action, ces derniers [les héritiers] doivent être regardés comme des » personnes concernées » au sens des articles 2 et 39 de la loi du 6 janvier 1978 pour l'exercice de leur droit d'accès aux données à caractère personnel concernant le défunt, dans la mesure nécessaire à l'établissement du préjudice que ce dernier a subi en vue de sa réparation et pour les seuls besoins de l'instance engagée. »*

Lire la décision

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>



Réagissez à cet article

Source : *Legalis | L'actualité du droit des nouvelles technologies | Condition de l'accès d'un héritier aux données d'une personne décédée*

L'utilisation des données personnelles : mine d'or ou danger ?

x	L'utilisation des données personnelles : mine d'or ou danger ?
---	--

Nos données personnelles sont utilisées par tout le monde, avec des buts très différents. Dans le domaine de la santé, « elles pourraient sauver des vies ». Dans le domaine privé, c'est dans un but lucratif qu'elles sont récoltées.

Le domaine de la santé regorge de données personnelles et de statistiques. Utilisées dans les orientations stratégiques, elles pourraient améliorer notre santé.

« La France est un des pays avec le plus de données de santé et qui les utilise le moins », assure Cédric Duboudin. Pour le directeur stratégique de l'Agence régionale de santé (ARS) Bourgogne Franche-Comté, « nous sommes assis sur une mine d'or ».

« Dans les systèmes anglo-saxons, il est possible, grâce aux données, de voir si les personnes atteintes de pathologies lourdes reçoivent le bon traitement. »

Pour l'instant, les données médicales des habitants de la région servent à « concevoir l'offre de soins de manière optimale », précise Didier Carel. « Où inciter les professionnels à s'installer, par exemple. » Une fois la décision prise, les statistiques permettent aussi d'évaluer les résultats.

Mais les données personnelles pourraient servir à bien plus, pour Cédric Duboudin.

✘ « On ne donne plus le même traitement selon le patient. Derrière un cancer pulmonaire, il y a des centaines de typologies. On peut acquérir des données très fines, comme les génomes de l'individu et de la tumeur. Cela peut poser des questions d'éthique, mais ces données personnelles permettront l'amélioration des traitements et de l'espérance de vie. »

Mais le ministère de la Santé reste limité par la CNIL, qui veille à ce qu'il n'y ait pas d'utilisation malveillante de ces données.

« Utiliser des données personnelles est important, il est différent de s'en servir à des fins de santé publique ou pour un but moins noble. Ces utilisations moins nobles amènent en place une législation qui nous contraint. »...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>




Réagissez à cet article


Source : *L'utilisation des données personnelles : mine d'or ou danger ? – Auxerre (89000) – L'Yonne Républicaine*


Téléchargement RGPD Règlement européen sur la protection des données (officiel) Replay-

✖	Téléchargement RGPD Règlement européen sur la protection des données (officiel)
---	--

Vous trouverez ici le lien direct sur le site de l'Union Européenne pour télécharger le 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.

La page du site de l'Union européenne 

Version française du règlement (UE) 2016/679 

English version of General Data Protection Regulation (UE) 2016/679 

A savoir : le règlement européen abroge la directive européenne 95/46/CE.

Quand le règlement européen sera-t-il applicable ?

Le règlement sera applicable à partir du 25 mai 2018 (article 99.2 du règlement) dans tous les pays de l'Union Européenne. Les fichiers déjà mis en oeuvre à cette date devront, d'ici là, être mis en conformité avec les dispositions du règlement.

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>



Réagissez à cet article

La sanction de la Cnil contre Optical Center confirmée par le Conseil d'Etat

x	La sanction de la Cnil contre Optical Center confirmée par le Conseil d'Etat
---	--

Le Conseil d'Etat a validé la sanction pécuniaire de 50 000 € que la Cnil avait prononcé à l'encontre d'Optical Center, le 5 novembre 2015, pour manquement à ses obligations de sécurité et de confidentialité, par une décision du 19 juin 2017. Il a en revanche réformé la délibération de la Cnil sur la mesure de publication, en raison de son absence de limite dans le temps.

Le Conseil d'Etat a, en effet, considéré que la sanction complémentaire infligée à l'opticien était excessive et a jugé que le maintien de la décision de la Cnil non anonymisée sur son site devait être limité à deux ans. Si la publication de la délibération vise à renforcer le caractère dissuasif de la sanction principale en lui assurant une publicité à l'égard du public, elle doit cependant respecter le principe de proportionnalité, rappelle le Conseil d'Etat.

Dans sa délibération du 5 novembre 2015, la formation restreinte de la Cnil avait considéré que la société ne s'était pas mise en conformité sur deux points qu'elle lui reprochait.

- D'abord, elle n'avait pas mis en place les mesures adaptées pour assurer la sécurité et la confidentialité des données des 170 000 comptes utilisateurs sur son site. La Cnil avait constaté que, malgré sa mise en demeure, la zone de saisie de l'identifiant et du mot de passe pour accéder au compte client depuis la page d'accueil n'était pas accessible depuis une page web sécurisée par le protocole https. A noter qu'Optical Center s'était quand même conformé à la demande de la Cnil de « *mettre en œuvre chiffrement du canal de communication et une authentification du site distant lors de l'accès au site web, que ce soit au stade de l'authentification des clients ou au stade du renseignement et de la validation du formulaire de collecte des données aux fins de création du compte* ».

- Par ailleurs, la formation restreinte avait sanctionné la société car le contrat signé avec l'un de ses sous-traitants ne contenait pas de clause précisant les obligations de ce prestataire en matière de protection de la sécurité et de la confidentialité des données des clients.

« *Eu égard à la nature, à la gravité et à la persistance des manquements constatés, la formation restreinte la CNIL n'a pas infligé à la société une sanction disproportionnée aux faits de l'espèce en prononçant à son encontre une sanction pécuniaire d'un montant de 50 000 euros.* », a jugé le Conseil d'Etat.

Cette sanction particulièrement sévère pour l'autorité de contrôle s'explique en partie, et comme souvent, par le manque de coopération, voire par la résistance de la personne ou de l'organisme épinglé, lors de l'instruction.

Lire la décision

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Legalis | L'actualité du droit des nouvelles technologies | La sanction de la Cnil contre Optical Center confirmée par le Conseil d'Etat*

198 millions de données personnelles d'Américains ont été exposées

	198 millions de données personnelles d'Américains ont été exposées
---	---

Un chercheur en cybersécurité a découvert, le 12 juin, 1 téraoctet d'informations issues de fichiers électoraux ou d'analyses de données, librement accessibles en ligne. Derrière la faille, une société qui compte le Parti républicain parmi ses clients.

Noms, prénoms, dates de naissance, adresses postales et mail, numéros de téléphone, affiliations politiques et origines ethniques autodéclarées : autant de données personnelles qu'accumulent les (très bavards) fichiers électoraux américains. Et dont les deux grands partis, et les entreprises spécialisées dans le *big data* ou le pilotage de campagne électorale, font leur miel. Or le 12 juin, Chris Vickery, chercheur pour l'entreprise de cybersécurité Upguard, a découvert qu'une telle base de données concernant 198 millions d'électeurs, soit près de 99% des inscrits, était librement accessible en ligne, sans identifiant ni mot de passe, dans un espace de stockage loué à Amazon... Aux informations issues des fichiers électoraux s'ajoutaient en outre des éléments «prospectifs» issus d'analyses de données : la religion supposée, mais aussi la probabilité d'avoir voté Obama en 2012, ou d'adhérer à la politique «*America First*» de Donald Trump...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article


Source : *Les données personnelles de 198 millions d'Américains ont été exposées – Libération*


Téléchargez le règlement européen sur la protection


des données (officiel)

	Téléchargez le règlement européen sur la protection des données (officiel)
---	---

Vous trouverez ici le lien direct sur le site de l'Union Européenne pour télécharger le 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.

La page du site de l'Union européenne 

Version française du règlement (UE) 2016/679 

English version of General Data Protection Regulation (UE) 2016/679 

A savoir : le règlement européen abroge la directive européenne 95/46/CE.

Quand le règlement européen sera-t-il applicable ?

Le règlement sera applicable à partir du 25 mai 2018 (article 99.2 du règlement) dans tous les pays de l'Union Européenne. Les fichiers déjà mis en oeuvre à cette date devront, d'ici là, être mis en conformité avec les dispositions du règlement.

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>



Réagissez à cet article