

Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI



Votre responsabilité engagée en cas de piratage de vos données

Les dispositifs biométriques utilisant le contour de la main des élèves pour gérer l'accès à la cantine scolaire sont couverts par une autorisation unique adoptée par la CNIL.

Les établissements qui souhaitent installer ce type de dispositifs doivent faire une déclaration simplifiée, en sélectionnant dans l'onglet « Finalité » l'autorisation unique AU-009.

Le responsable du dispositif s'engage ainsi à se conformer aux caractéristiques décrites dans ce texte.

Les autres dispositifs biométriques (réseaux veineux, empreintes digitales, reconnaissance faciale, etc.) doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=D5FEF7DD5664BF01E19E95AF8AF7782F>

Utilisation des photos des élèves : faut-il l'accord des parents ? | Denis JACOPINI

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>Utilisation des photos des élèves : faut-il l'accord des parents ?</h2>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------

Toute personne dispose sur son image et sur l'utilisation qui en est faite d'un droit exclusif et peut s'opposer à sa reproduction et à sa diffusion.

Si un établissement scolaire veut utiliser les photographies de ses élèves dans le journal de l'école, sur un trombinoscope ou sur son site, il doit donc obligatoirement obtenir le consentement des parents ou représentants légaux des mineurs. Cet accord doit être écrit. De plus, le traitement informatique des photographies (numérisation, diffusion à partir d'un site web, etc.) doit être déclaré auprès de la CNIL, sauf si l'établissement a désigné un Correspondant Informatique et Libertés (CIL).

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : <http://www.aide.cnil.fr/selfcnil/site/template.do?id=272&back=true>

Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur ?



Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur ?

Ne pas effacer ses données personnelles sur son ordinateur de fonction est-il dommageable (risque d'accès à nos données personnelles, vol d'identité ou accès frauduleux etc...)? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :

- Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix ;
- Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox... ;
- Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité. Même si l'article 226-4 du code pénal complété par la loi LOPPSI du 14 mars 2011 d'un article 226-4-1, l'usurpation d'identité numérique est un délit puni de deux ans d'emprisonnement et de 20 000 euros d'amende, il sera fastidieux d'une part pour vous, de prouver que vous n'êtes pas le véritable auteur des faits reprochés, et difficile pour les enquêteurs de retrouver le véritable auteur des faits.

Ne pas effacer ses données personnelles sur l'ordinateur que l'on rend, donne, vend, c'est laisser l'opportunité à un inconnu de fouiller dans vos papier, violer votre intimité et cambrioler votre vie.

Pire ! vous connaissez bien le donataire de votre matériel et vous savez qu'il n'y a aucun risque qu'il ait des intentions répréhensibles. Mais êtes vous certain qu'il sera aussi prudent que vous avec son matériel ?

Êtes-vous prêt à prendre des risques s'il perdait ce matériel ?

Dormiriez-vous tranquille si vous imaginiez que votre ancien ordinateur est actuellement sous l'emprise d'un pirate informatique prêt à tout pour tricher, voler et violer en utilisant votre identité ?

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaque**s et les **piratages informatiques** pour mieux s'en protéger et se mettre en conformité avec la **CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?



Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé (effacer l'historique de ses comptes mails et personnelles, formatage complet, logiciel d'aide à la suppression etc..) ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage.

- Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :
- Des programmes ajoutés ;
 - Nos e-mails ;
 - Nos traces de navigation ;
 - Nos fichiers téléchargés ;
 - Divers identifiants et mots de passe ;
 - Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés

Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :

- soit par le raccourci de désinstallation que le programme a créé ;
- s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;

• Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevõInstall (gratuit).

Concernant les e-mails

Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :

- fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
- fichiers dans « %AppData%\Microsoft\Windows Live Mail » pour le logiciel « Windows Live Mail » ;
- les fichiers contenus dans « %APPDATA%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird
- le dossier contenu dans « ..Local Settings\Application Data\IMIdentities » pour le programme IncrediMail.

Concernant nos traces de navigation

En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés

En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe

Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ». Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passe et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires

En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).

En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir

Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore ».

Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84). Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement. Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis Jacopini est Expert Informatique assurément spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (piratage, fraude, arnaque, espionnage, cambriolage, contrefaçon, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté);
- Accompagnement à la mise en conformité CNIL de votre Etablissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée – ZDNet

Étape par étape : comment bien effacer et conserver vos données informatiques

stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?



Étape par étape comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?

Original de l'article mis en page : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) | Atlantico.fr

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Denis JACOPINI



Denis JACOPINI

VOUS INFORME

LCI

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Denis JACOPINI

Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « ilfaitbeaudanstoutelafrancesaufdanslebassinparisien » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « p8)J#&=89pE », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que la phrase choisie comme mot de passe ne soit pas une phrase connue de tous, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « Sur le pont d'Avignon, on y danse on y danse... ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « jevaispromenermonchienTITIdansle93 ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. Dès lors, plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui vérifie nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien vérifier son ordinateur, etc...

Article original de Denis JACOPINI et Atlantico

Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Original de l'article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Atlantico.fr

La CNIL et la CADA publient un guide pratique



La Commission nationale de l'informatique et des libertés (CNIL) et la Commission d'accès aux documents administratifs (CADA), en partenariat avec les services d'Etalab, ont annoncé la publication d'un guide pratique de la publication en ligne et de la réutilisation des données publiques.

Ce guide est composé d'une présentation du cadre juridique et d'une fiche pratique sur l'anonymisation. Ce document fait suite à une consultation publique qui s'est tenue au printemps 2019, afin « de confronter les travaux engagés pour la présentation du cadre juridique de l'open data aux attentes concrètes des acteurs concernés ». 220 contributions ont été enregistrées. « Son succès témoigne tant de l'intérêt du public porté à la question de l'open data que du besoin d'accompagnement des administrations diffusant en ligne des données publiques ainsi que des réutilisateurs de ces données », se félicitent les partenaires....[lire la suite]

Téléchargez le guide.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE



Datadock
Organisme validé
et référencé

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

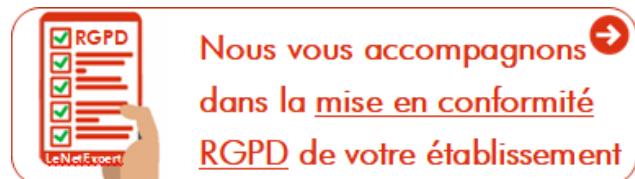
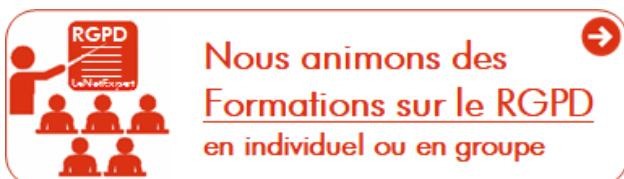
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une expérience d'une dizaine d'années dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisément d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

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

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

Comprendre le Règlement Européen sur les données personnelles

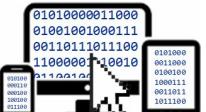
en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source : *Open data : la CNIL et la CADA publient un guide pratique – Image – CB News*

RGPD : quel impact sur les établissements scolaires ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LE NET EXPERT .fr	 RGPD CYBER LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI vous informe	RGPD : quel impact sur les établissements scolaires ?				

Entré en vigueur le 25 mai 2018, le Règlement Général de Protection des Données (RGPD) promet une protection des données personnelles à l'échelle européenne. Dès lors, tous les secteurs sont confrontés à de nouveaux enjeux, y compris les institutions publiques telles que les établissements scolaires.

Données personnelles à l'école : théorie vs pratique Si le RGPD change la donne pour bon nombre d'acteurs, l'environnement pédagogique avait déjà sa propre réglementation en matière de digital. En effet, l'arrêté du 30 novembre 2006, modifié par l'arrêté du 13 octobre 2017, définit l'acte réglementaire unique RU-003 destiné à régir la mise en place et l'exploitation des Espaces Numériques de Travail dans l'ensemble de l'écosystème scolaire,...[lire la suite]

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



DÉSIGNATION
N° DPO-15945



Data**dock**
Organisme **validé**
et **référencé**

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

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisément d'accompagner les organismes dans leur démarche de mise en conformité avec le RGPD.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Nous animons des Formations sur le RGPD
en individuel ou en groupe



Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

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

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

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)

[block id="24761" title="Pied de page HAUT"]

Source : RGPD : quel impact sur les établissements scolaires ?
– Les Echos

Données personnelles : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »



The image is a screenshot of a television news program. In the top left corner, the channel logo 'LE JT' is displayed with the number '8'. To the right of the logo is a small portrait of a man, identified as Denis JACOPINI. Below the logo, there is a blue banner with white text that reads 'DENIS JACOPINI PAR TÉLÉPHONE EXPERT INFORMATIQUE ASSURÉMENT APPROUVE DES FORMATION VS MONSIEUR PIRATE PARISIMA CONSULTANT'. At the bottom of the screen, the text 'vous informe' is written in large blue letters.

RGPD : Les collectivités vont devoir se lancer dans une démarche de mise en conformité

Article original : La gazette des communes

A un an de l'entrée en vigueur du règlement européen sur la protection des données, Alice de La Mure, juriste au service Correspondants informatiques et libertés de la CNIL, revient sur les nouvelles obligations qui concernent largement les collectivités territoriales.

Le règlement général sur la protection des données (RGPD), adopté par le Parlement européen le 14 avril 2016, sera directement applicable dans les Etats membres le 25 mai 2018. Il sera alors le texte de référence concernant la protection des données à caractère personnel. Il consolide, voire renforce, les grands principes de la loi Informatique et Libertés.

Divers axes s'en dégagent, dont plusieurs concernent directement les collectivités territoriales :

- la responsabilisation globale de l'ensemble des acteurs ;
- le renforcement des droits des personnes, avec notamment l'avènement du droit à la portabilité et du droit à la limitation du traitement ;
- l'augmentation du montant des sanctions susceptibles d'être prononcées par la CNIL : la loi du 7 octobre 2016 pour une République numérique avait ...[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



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 : *Données personnelles : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »*