# Les obligations des Associations vis à vis de la CNIL | Denis JACOPINI



Les obligations des Associations vis à vis de la CNILDans le cadre de leur activité, les associations sont amenées à constituer des fichiers de leurs adhérents, de leurs donateurs ou de donateurs potentiels. Quelles sont les règles à respecter ?

Dans le cadre de leur activité, les associations sont amenées à constituer des fichiers de leurs adhérents, de leurs donateurs ou de donateurs potentiels. Quelles sont les règles à respecter ?

Nous allons tenter d'y répondre au travers de réponses par Oui ou par Non à des questions correspondant à des cas concrets : Une association peut-elle céder, louer ou vendre le fichier de ses adhérents à des fins commerciales ?

OUI. La loi « informatique et libertés » n'interdit pas cette pratique. Il y a toutefois des précautions à prendre : Il faut d'abord informer les adhérents de cette possible revente de leurs coordonnées à des fins commerciales et leur permettre de s'y opposer. Cette opposition peut se faire par exemple au moyen d'une case à cocher figurant sur le bulletin d'adhésion.

## Une association peut-elle diffuser sur son site web l'annuaire de ses adhérents ?

OUI. Dans ce cas, comme pour la réponse précédente, les adhérents doivent en être informés au préalable. Ils ont tout à fait le droit de s'opposer à une telle diffusion compte-tenu des risques particuliers de capture des informations diffusées sur le web.

La CNIL propose des mentions type à faire figurer sur les bulletins d'adhésion pour bien informer les adhérents de leurs droits.

#### Mention d'information à inscrire sur le bulletin d'adhésion

Les informations recueillies sont nécessaires pour votre adhésion. Elles font l'objet d'un traitement informatique et sont destinées au secrétariat de l'association. En application des articles 39 et suivants de la loi du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

#### Il arrive que des mairies demandent aux associations de leur transmettre le fichier de ses adhérents en vue d'obtenir des subventions ? Est-ce légal ?

NON. Un maire ne peut pas demander, même au titre de la subvention qu'il accorde à une association, la liste nominative des adhérents. Une telle pratique est contraire au principe constitutionnel de la liberté d'association.

En revanche, les mairies peuvent demander, au titre du contrôle des subventions qu'elles versent aux associations, la copie certifiée du budget et des comptes de l'exercice écoulé, ainsi que la communication de tous les documents faisant apparaître les résultats de l'activité de l'association.

## Un membre d'association peut-il exiger la communication de la liste de tous les autres adhérents ?

OUI, si les statuts de l'association prévoient cette possibilité. Une association est en effet libre de préciser dans ses statuts que l'adhésion implique d'accepter que ses coordonnées puissent être communiquées à tout adhérent qui en fait la demande, à la condition que cette communication ait un lien direct avec l'activité de l'association.

Dans ce cas, un membre ne peut s'opposer à cette diffusion.

# Lors du renouvellement du bureau d'une association, un candidat peut-il obtenir la liste des adhérents ?

OUI. Si les statuts de l'association le prévoient, tout candidat peut demander que la liste des adhérents lui soit transmise, à partir du moment où il s'engage à ne pas l'utiliser à d'autres fins que l'élection et à la détruire à la fin des opérations électorales.

Les membres du bureau d'une association, dont les statuts ont été déposés en préfecture, peuvent ils s'opposer à la

#### diffusion de leurs identités et coordonnées ?

NON. La loi du 1er juillet 1901 relative au contrat d'association prévoit qu'une association ne peut obtenir la capacité juridique qu'en rendant publics, par une insertion au Journal officiel, son titre, son objet, l'adresse de son siège et les noms, professions, domiciles et nationalités de ceux qui sont chargés de son administration. Cette diffusion peut aussi se faire sur en ligne via la version Internet du journal Officiel.

Néanmoins, des mesures techniques empêchent d'accéder directement à la page de l'association concernée lorsqu'on interroge les différents moteurs de recherche sur la base de l'identité des membres de son bureau.

### Les fichiers de membres et donateurs d'une association doivent-ils être déclarés à la CNIL ?

NON, ces fichiers sont dispensés de déclaration à la CNIL.

Attention, être dispensé de déclaration n'exonère pas pour autant des obligations que la loi informatique et libertés impose aux responsables de fichiers. Cela signifie qu'il faut informer les personnes qu'un fichier est constitué et qu'elles ont un droit d'accès aux informations qui les concernent. Enfin bien sûr, le responsable du fichier doit prendre toutes les mesures utiles afin d'assurer la sécurité des informations personnelles collectées.

Source : Denis JACOPINI et www.cnil.fr

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Règlement européen sur la protection des données : Renforcement des droits des personnes

Règlement européen sur la protection des données : Renforcement des droits des personnes

#### Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci. Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

#### De nouveaux droits

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

source : CNIL



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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

### 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 quittérais on travail et que l'on ne sombaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit blane effacé d'effacer l'historiume de sex converts mails et nerradace commelte. Formatace commelte. Organisace commeltes de conversion 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 • Nes 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
uppression, nous vous conseillons de procéder :
soit par le raccourcis de désinstallation que le programme a créé ;
s'il n'y a pas de raccourcis de désinstallation que le programme a créé ;
s'il n'y a pas de raccourcis prévuà ècet 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 Revoluninstaller (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 seton (e programme vost » de votre compte et archives pour le logiciel « Outlook » ;

\*\*Supprimer\*\*

\*\*Ichters dans « » » "ApphatalocalNicrosoftWindoos Live Mail » pour le logiciel « Windoos Live Mail » ;

\*\*Les fichiers contenus dans " » » "APPANTANThunderbirdProfiles » pour le programme Mozilla Thunderbird

\*\*Le dossier contenus dans « ..Local SettingsApplication basalMidentities » 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 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 vote ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de
passes et les informations qui pré remplissent les champs. 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°38 88 030401 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les armaques 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.lenetexport.fr/formations-cybercrismaintie-protection-des-données-personnelles Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des demées personnelles. contentious, detoumements de cardentele...);

• Expertises de systèmes de vota dénéronique;

• Formations et conférences en cybercriminalité;

• Formation de C.I.I. (Correspondants Informatique et Libertés); Le Net Expert

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

# Quelles formalités une pharmacie doit déclarer à la CNIL ? | Denis JACOPINI



# Ouelles formalités une pharmacie doit déclarer à

Les fichiers relatifs à la gestion d'une pharmacie doivent être déclarés à la CNIL :Par une déclaration simplifiée de conformité à la norme n°52 si le fichier correspond aux caractéristiques énoncées dans ce texte ;

Par une déclaration normale si le fichier sort du cadre de cette norme.

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 plait ? Partagez ! Un avis ? Laissez-nous un commentaire !

Source .

http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=193E337DAA685A15B25C9E90E19E80BF?name=Activit%C3%A9+d%27une+pharmacie+%3A+quelles+formalit%C3%A9s+%C3%A0+la+CNIL+%3F&id=545

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) ?



Etape 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)?

Quitter son travail est souvent difficile, mais effacer des données présentes sur un ordinateur professionnel sur lequel on a travaillé pendant X années l'est encore plus. Il est donc nécessaire de savoir

Atlantico : Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction

Demis Jacopini : L'ordinateur professionnel qui vous a été mis à disposition était probablement en état de marche. A moins d'avoir des circonstances ou des consignes particulières, vous devrez donc rendre cet appareil au moins dans l'état initial.

Le de propriet au musin dans telat initiat.

1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients.

On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.

- 2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hachage.

- 3. Identifier les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre...
  4. Identifier les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants...)
  5. Identifier les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ça soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifier les fonctions de « Sauvegarde », « Enregistrer sous » ou d' »Export ». Vous pourrez alors choisir le support adapté.

Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptée soit :

- Entlin, en fonicion des Ciletes de Securice Choisis, vous pour les sauvegators sur des supports adaptée soit :

   à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hachage tel de Truecrypt, Veracrypt, ou AxCrypt...);

   à l'intégrité (multiplier le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à n'absolument pas perdre);

   à la longévité en utilisant des supports avec une durée de vie adapté à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une information numérique au-delà de plusieurs dizaines d'années (en raison de l'altération des supports avec le temps, mais aussi de l'évolution des versions, des formations et des logiciels). Qui peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
- à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions cloud qui sont éclos il y a quelques dizaines d'années seulement ;

   à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions cloud qui sont éclos il y a quelques dizaines d'années seulement ;

   à la quantité (car vous devez rapidement stocker pour ensuite trier et choisir un support adapté) en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

#### Les risques :

Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tomberont un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.

Idem pour les disques durs. 100% des disques durs tomberont un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus

Tacilement de récupérer leur contenu en cas de panne.

Les supports de type lecteurs ZIP, lecteur JAZ, lecteurs magnéto-optiques, lecteurs de bandes etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant jour ou vous souhaitez y accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vies de vos données numériques entre les mains du Bon Coim.

Voilà, en fonction de tous ces critères et à partir de ces conseils, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Disque dur : Quelques Go à quelques To — Bon marché, rapide mais fragile.

Disque dur : Quelques Go à quelques To — Bon marché, rapide mais fragile.

Clé USB : Quelques Go — Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.

Cloud : Quelques Mo à quelques To — Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) — Dépend du fonctionnement et de la rapidité d'Internet — Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdrez tout.

Disques optiques (CD, DVD, Magnéto Optique) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (pérennité des lecteurs de disques) jusqu'à quand ?

Supports spéciaux (ZIP/Jazz/OIC/DAT/DIDS/SDIT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au dela de 5 ans.

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 traces sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé

?

. 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 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

ammes installés. Pour procéder à leur suppression, nous vous conseillons de procéder : t par le raccourcis de désinstallation que le programme a créé ; l 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)

d'exploitation de sa version);
— Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (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 » » « » "AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
— les fichiers contenus dans ' » » « » "APPDATAWThunderbirdProfiles » pour le programme Mozilla Thunderbird
— le dossier contenu dans « \_Local SettingsApplication DataIMIdentities » 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 :

Concernant des richiers telecharges:
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 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

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 recommêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs. andons d'utiliser les fonctions dans ces 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

Todar - Land - 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 monque supprime mais l'experiment de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore ».

  Ne pas effacer ses données personnelles sur so ordinateur de fonction est-il dommageable ? 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 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.

Auteur : Denis JACOPINI

Denis Jacopini anime des conférences et des formations 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 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.

- Formations et conférences en cybercriminalité ; Formation de C.I.L. (Correspondants Informatique et Libertés);



Contactez-nous

Réagissez à cet article

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

Sensibilisations et Formations à la Cybercriminalité et au RGPD (Protection des données personnelles) — Redirect

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment (Intervention en France et étranger)

Nos formations sont personnalisées en fonction du type de publics présent (Dirigeants, cadres , informaticiens, responsable informatique, RSSI, utilisateurs).

Contactez-nous

#### **PROGRAMME**

#### **CYBERCRIMINALITÉ**

# COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

#### Présentation

La France a rattrapé sont retard en matière d'équipement à Internet mais à en voir les dizaines de millions de français victimes chaque année, les bonnes pratiques ne semblent toujours pas intégrées dans vos habitudes.

Piratages, arnaques, demandes de rançons sont légions dans ce monde numérique et se protéger au moyen d'un antivirus ne suffit plus depuis bien longtemps.

Avons-nous raison d'avoir peur et comment se protéger ?

Cette formation couvrira les principaux risques et les principales solutions, pour la plupart gratuites, vous permettant de protéger votre informatique et de ne plus faire vous piéger.

#### <u>Objectifs</u>

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant de naviguer sur Internet en toute sécurité.

Demande d'informations

#### **CYBERCRIMINALITÉ**

#### LES ARNAQUES INTERNET A CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

#### <u>Présentation</u>

Que vous vous serviez d'Internet pour acheter, vendre, télécharger ou communiquer, un arnaqueur se cache peut-être derrière votre interlocuteur.

Quels sont les signes qui ne trompent pas ? Comment les détecter pour ne pas vous faire piéger ?

#### **Objectifs**

Découvrez les mécanismes astucieux utilisés par les arnaqueurs d'Internet dans plus d'une vingtaine cas d'arnaques différents. Une fois expliqués, vous ne pourrez plus vous faire piéger.

#### Demande d'informations

#### PROTECTION DES DONNÉES

# RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) — CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

#### <u>Présentation</u>

Le Règlement Général sur la Protection de Données (RGPD) est entré en application le 25 mai 2018 et toutes les entreprises, administrations et associations ne se sont pas mises en conformité. Or, quelle que soit leur taille, elles sont toutes concernées et risqueront, en cas de manquement, des sanctions financières jusqu'alors inégalées.

Au delà de ces amendes pouvant attendre plusieurs millions d'euros, de nouvelles obligations de signalement de piratages informatiques risquent désormais aussi d'entacher votre réputation. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

Cette formation non seulement répondra la plupart des

questions que vous vous posez, vous offrira des éléments concrets non seulement pour initier la mise en conformité de votre établissement mais surtout pour transformer ce qui peut vous sembler à ce jour être une contrainte en une véritable opportunité.

#### **Objectifs**

Cette formation a pour objectif de vous apporter l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD dans le but à la fois de répondre à la réglementation et de prévenir en cas de contrôle de la CNIL.

Informations complémentaires

Demande d'informations

#### PROTECTION DES DONNÉES

# RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) — ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

#### <u>Présentation</u>

Après avoir suivi notre formation vous permettant de comprendre l'intérêt d'une telle réglementation et de savoir ce qu'il faut mettre en place pour bien démarrer, vous souhaitez aller plus loin dans la démarche de mise en conformité avec le RGPD.

Après un retour éclair sur les règles de base, nous ferons un point sur la démarche de mise en conformité que vous avez initiée ces derniers mois dans votre établissement. Nous détaillerons ensuite les démarches à réaliser en cas de détection de données sensibles et d'analyse d'impact. Enfin, nous approfondirons des démarches périphériques essentielles pour répondre à vos obligations.

#### **Objectifs**

Après avoir déjà découvert l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD, cette formation aura pour objectif de vous perfectionner afin de devenir référent protection des données ou DPO (Data Protection Officer = Délégué à la Protection des Données).

Demande d'informations

#### CYBERSÉCURITÉ DÉTECTER ET GÉRER LES CYBER-ATTAQUES

#### Présentation

Que vous ayez déjà été victime d'une cyber-attaque ou que vous souhaitiez l'anticiper, certaines procédures doivent absolument être respectées pour conserver un maximum de preuves et pouvoir les utiliser.

#### <u>Objectifs</u>

Que votre objectif soit de découvrir le mode opératoire pour savoir quelles sont les failles de votre système ou si vous avez été victime d'un acte ciblé avec l'intention de vous nuire, découvrez les procédures à suivre.

Demande d'informations

#### **CYBERSÉCURITÉ**

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ

#### SUR VOTRE SYSTÈME INFORMATIQUE

#### Présentation

Votre système informatique a très probablement de nombreuses vulnérabilités présentées aux pirates informatiques comme de nombreux moyens de nuire à votre système informatique.

Avant de procéder à un test d'intrusion, apprenez à réaliser l'indispensable audit sécurité de votre système informatique afin d'appliquer les mesures de sécurité de base présentes dans les référentiels internationalement utilisés.

#### **Objectifs**

Vous apprendrez au cours de cette formation la manière dont doit être mené un audit sécurité sur un système informatique, quelques référentiels probablement adaptés à votre organisme et nous étudierons ensemble le niveau de sécurité informatique de votre établissement.

Demande d'informations

#### **CYBERSÉCURITÉ**

#### APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

#### Présentation

Cette formation vous apporte l'essentiel de ce dont vous avez besoin pour adopter l'approche du Hacker pour mieux s'en protéger en élaborant vos tests de vulnérabilité, mettre en place une approche offensive de la sécurité informatique permettant d'aboutir à une meilleure sécurité et réaliser des audits de sécurité (test d'intrusion) au sein de votre infrastructure.

La présentation des techniques d'attaques et des vulnérabilités potentielles sera effectuée sous un angle « pratique ».

#### **Objectifs**

Cette formation vous apportera la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités les plus critiques pour mieux vous protéger d'attaques potentielles.

#### Demande d'informations

#### QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale, Investigation numérique pénale, et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.

A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur : http://www.leNetExpert.fr/contact





# Les données personnelles des portables d'occasion toujours accessibles | Denis JACOPINI



Les données personnelles des portables d'occasion toujours accessibles

De nombreux smartphones reconditionnés contiennent toujours des informations sensibles sur leurs anciens propriétaires.

Avant de revendre votre portable, veillez à bien effacer toutes vos données personnelles. En effet, de nombreux smartphones reconditionnés — c'est-à-dire d'occasion et revendus dans les boutiques — contiennent toujours des informations de leurs anciens propriétaires, selon une étude réalisée par l'entreprise Avast, spécialisée dans les antivirus, et révélée en exclusivité par Europe 1.

Emails, photos, SMS, factures personnelles ou même clichés à caractère sexuel : ces téléphones renferment souvent des données extrêmement sensibles.

#### Un contrat de travail, des mails et des SMS retrouvés

Le problème concerne une part croissante du marché des téléphones portables. 10% des Français ont en effet acheté un mobile de seconde main en 2015. Avast a ainsi mené une expérimentation sur vingt anciens modèles de smartphone, achetés à New York, Paris, Barcelone et Berlin. Les résultats sont édifiants : sur cet échantillon test, de nombreuses données personnelles ont été retrouvées.

Avast a ainsi pu accéder à 2.000 photos, dont des clichés d'enfants, d'autres à caractère sexuel, mais aussi un contrat de travail ou encore 300 mails et SMS. Pire : deux propriétaires de téléphone avaient oublié de déconnecter leurs comptes Gmail, prenant le risque que les nouveaux acheteurs lisent ou envoient des mails en leur nom.

#### « Important de faire une démarche complète »

Bien que 40% des portables vendus dans les boutiques d'occasion soient reconditionnés, les anciens propriétaires réinitialisent souvent mal, voire pas du tout, leurs terminaux. Les revendeurs spécialisés le constatent ainsi tous les jours. « Ça arrive à un client sur deux : quand il nous propose son téléphone, il ne l'a pas effacé au préalable », explique Frédéric Bertinet, de Cash Express.

« Les téléphones ont été mal réinitialisés, donc on pense qu'on a fait le travail parce qu'on a enlevé les mots de passe et les réglages, mais le contenu lui n'a pas été effacé. Il est important de faire une démarche complète, un peu procédurière », conclut Frédéric Bertinet.

#### Des applications sécurisées pour effacer les données

Mais pour éviter tout risque, une simple réinitialisation ne suffit pas. « Lorsqu'un fichier est effacé, c'est seulement la référence de ce fichier qui disparaît. Pour que ces fichiers disparaissent complètement, il faut les remplacer par d'autres données quelconques, c'est-à-dire des 0 et des 1. Sinon, c'est théoriquement récupérable », détaille Arnaud Matthieu, représentant d'Avast pour la France.

Pour vider à jamais votre téléphone portable, des applications sécurisées sont disponibles gratuitement sur Internet. Mais attention : si vous n'écrasez pas correctement vos données personnelles, les risques sont immenses. Les anciens propriétaires de smartphones s'exposent à du chantage, à des photos personnelles publiées sur internet ou encore à de l'usurpation d'identité.



Réagissez à cet article

Source : Les données personnelles des portables d'occasion toujours accessibles

# Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité | Denis JACOPINI

Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité

Pour information, Denis JACOPINI propose depuis quelques mois deux nouveaux sujets de formation à destination des chefs d'entreprise, de leurs salariés mais aussi des administrations et de leurs agents :

- La cybercriminalité, un vrai risque pour les chefs d'entreprises Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi
- Cybercriminalité, sécurité informatique et CNIL, bonnes pratiques et cadre juridique
- La cybercriminalité, un vrai risque pour administrations

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

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire…

# Règlement européen sur la protection des données : Evolution du cadre juridique

Règlement européen sur la protection des données : Evolution du cadre juridique

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne le 4 mai 2016 et entré en application le 25 mai 2018. L'adoption de ce texte permet à l'Europe de s'adapter aux nouvelles réalités du numérique

Un cadre juridique unifié pour l'ensemble de l'UE Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du rèalement.

#### Un champ d'application étendu

#### · Le critère du ciblage

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par

#### · La responsabilité des sous-traitants

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le projet de règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

#### Un guichet unique : le « one stop shop »

Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements

#### Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement sera transnational — donc qu'il concernera les citoyens de plusieurs États membres —, les autorités de protection des données des différents États concernées seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file »

• Par exemple, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État. Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

source : CNIL





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);



Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur



Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur Contacted preferation of source sour difference as dones preferation and extended to all the contractions of the contact interpretation of personality (or contact of personality). Contacted preferations of our anything discontinuous and an activation of the contact of the con

Original de l'article mis en page : Supprimer vos données personnelles avant de donner ou recycler un ordi — FrancoisCharron.com