

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

Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction (sauvegarder des fichiers importants et personnelles (contacts importants, copier des fichiers et tout ce qui nous concerne (photo, pdf, CV etc...)) sur un disque dur ou un système de Cloud etc...)?

- 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.
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 hashage.
 3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre...
 4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits enfants...)
 5. Identifiez 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, identifiez 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 :

- à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hashage 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 adaptée à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une informations 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 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 facilement 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 coin...

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.

Comparatif

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/QIC/DAT/DLT/DOS/SDLT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au delà de 5 ans.

Denis JACOPINI anime des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux CyberRisques.
Il est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant a une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.
<http://www.leetexpert.fr/contact>
<https://twitter.com/lenetexpert>
<https://www.linkedin.com/in/lenetexpert>



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

- Expertises techniques (virus, espions, pièges, fraudes, attaques Internet...) et judiciaires (investigation téléphones, disques durs, e-mails, contenus, échantillonnage de données...);
- 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 établissement.



Contactez-nous

Réagissez à cet article

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

RGPD : Faire face aux exigences



Denis JACOPINI

vous informe

RGPD : Faire face aux exigences

À compter du 25 mai 2018, le nouveau règlement européen relatif à la protection des données personnelles connu sous l'acronyme RGPD s'appliquera à toutes les entreprises publiques ou privées.

Ces dernières devront entrer dans une démarche proactive de mise en conformité du nouveau règlement. L'enjeu est de taille, car tout manquement à ces nouvelles obligations pourrait être lourdement sanctionné par l'autorité de contrôle, la CNPD, qui sera habilitée dès l'entrée en vigueur du règlement à infliger des amendes allant jusqu'à 20 millions d'euros et 4 % du chiffre d'affaires mondial.

Le champ d'application du RGPD est particulièrement large : toutes les entités, européennes ou non, sont concernées à partir du moment où elles collectent et effectuent des traitements de données à caractère personnel d'un citoyen européen. Le RGPD vient renforcer les droits de la personne, et par conséquent augmenter les devoirs et les responsabilités de toute la chaîne d'acteurs, du responsable de traitement aux partenaires commerciaux, y compris les sous-traitants fournisseurs de services. Tous les flux de données sont concernés par cette nouvelle réglementation.

Ces nouvelles contraintes s'appuient notamment sur le principe d'accountability qui impose à chaque entreprise une obligation de rendre compte, notamment en se dotant d'une politique globale de protection des données conforme à la réglementation, et en étant à même de prouver à tout moment que des mesures concrètes et des procédures adéquates ont été mises en place. Dans ce nouveau contexte, il est préconisé que les responsables de traitement aient recours à des prestataires externes leur permettant d'assurer une mise en conformité effective...[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 ;
- Formation de la DCTE (PDS 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous



Réagissez à cet article

Source : «*Faire face aux exigences posées par le RGPD*» | Paperjam News

Quelques conseils pratiques pour assurer la sécurité de

vos systèmes informatiques

 Denis JACOPINI VOUS INFORME L'CI	Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques
---	---



Original de l'article mis en page : Conseils aux usagers |
Gouvernement.fr

Comment sécuriser Firefox efficacement en quelques clics de souris ?

 Attention, danger ! La modification de ces préférences avancées peut être dommageable pour la stabilité, la sécurité et les performances de cette application. Ne continuez que si vous savez ce que vous faites. ☒ Afficher cet avertissement la prochaine fois Je ferai attention, promis !	Comment sécuriser Firefox efficacement en quelques clics de souris ?
--	---

Vous utilisez Firefox et vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimeront la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande `about:config`. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne `security.tls.version`. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne `geo.enabled` pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaissent pas la dernière page que vous avez pu visiter, cherchez la ligne `network.http.sendRefererHeader` et mettez la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne `browser.safebrowsing.malware.enabled`.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne `browser.safebrowsing.provider.google.lists` et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offline », en mode hors connexion. Cherchez les lignes `offline-apps.allow_by_default` et `offline-apps.quota.warn`. La première valeur est à passer en False, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal



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 : Sécuriser Firefox efficacement en quelques clics de souris – Data Security BreachData Security Breach

RGPD : Impact sur l'Email Marketing



En mai 2018 entrera en vigueur le fameux RGPD : le Règlement Européen sur la Protection des Données. Il vise avant tout à renforcer la protection des données personnelles des internautes. De nombreux articles en ont déjà parlé et beaucoup imaginent que cette réglementation touchera de plein fouet les acteurs de l'email marketing français et leurs utilisateurs.

Sarbacane Software propose une infographie* résumant les réels changements qui seront apportés par le RGPD, et son implication pratique dans le domaine de l'emailing.



[lire la suite]

LE NET EXPERT

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

Besoin d'un Expert ? contactez-nous

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

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD ;**
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contenus, détournements de clients... ;
- **Expertises de systèmes de vote électronique ;**



Contactez-nous



Réagissez à cet article

Source : Sarbacane : Tout comprendre sur le RGPD, le règlement européen qui va impacter toutes les entreprises en 2018 – Global Security Mag Online

et Sarbacane.com

L'adresse IP est-elle une donnée à caractère personnel ? | Denis JACOPINI

 Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité vous informe...	L'adresse IP est-elle une donnée à caractère personnel ?
---	--

La nature juridique de l'adresse IP ne cesse de susciter les interrogations. Si la réponse à cette question semble a priori tranchée par la loi 6 janvier 1978 modifiée en 2004 en prévoyant une définition large de la donnée personnelle permettant d'inclure aisément des données numériques à partir du moment où elles permettent d'identifier même indirectement la personne physique, ainsi que par la CNIL qui s'est prononcée en faveur à cette assimilation, la jurisprudence quant à elle, ne cesse de changer de position, tantôt elle prône pour cette qualification, tantôt elle la rejette catégoriquement.

I/ L'adresse IP au regard de la loi du 6 janvier 1978.

L'article 2 alinéa 2 de la loi du 6 janvier 1978, dite loi informatique et libertés telle que modifiée par la loi du 6 août 2004, définit la donnée personnelle comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

Par cette vague définition, le législateur, conscient de l'évolution rapide et constante des nouvelles technologies, a sciemment élargi la définition de la donnée personnelle afin d'y inclure toute nouvelle donnée qui est susceptible d'identifier directement ou indirectement une personne physique, dans le but de la protéger.

Ainsi, dans cet éventail d'informations, peuvent se glisser aussi bien des informations personnelles « classiques » telles que le nom, prénom, adresse postale, photo, numéro de téléphone, empreintes digitales etc, que des informations du monde numérique. Tel est le cas de l'adresse IP (Internet Protocol) d'un ordinateur.

Toutefois, le fait de ne pas dresser une nomenclature des informations qui constituent les données à caractère personnel, présente la souplesse d'inclure de nouvelles données, mais l'absence d'une telle précision laisse planer le doute en cas de conflit, d'où le nombre d'affaires porté devant les tribunaux et dont la qualification est laissée à l'appréciation des juges.

Interrogée sur cette question, la CNIL (Commission Nationale Informatique et Libertés), à travers ses interventions (recommandation ou déclaration), a répondu favorablement à la reconnaissance de l'adresse IP comme une donnée à caractère personnel en se basant sur la définition large de l'article 2 de la loi du 6 janvier 1978 précitée.

II/ L'adresse IP selon les recommandations de la CNIL.

Dans un article du 2 août 2007, la CNIL [1] [2] comme le G29 [3] ont soutenu que l'adresse IP, à l'instar d'une plaque d'immatriculation d'un véhicule ou d'un numéro de téléphone, entre dans le champ d'application large de la définition de l'article 2 de la loi du 6 janvier 1978 modifiée étant donné qu'elle permet l'identification directe ou indirecte de la personne physique [4]. La CNIL a rappelé à ce titre, que l'ensemble des autorités de protection des données des Etats membres ont précisé dans un avis du 20 juin 2007 relatif au concept de données à caractère personnel que l'adresse IP liée à l'ordinateur d'un internaute constitue une donnée à caractère personnel. S'inquiétant ainsi des décisions judiciaires qui refusent de considérer cette donnée comme personnelle. L'évolution récente de la jurisprudence va dans ce sens.

III/ L'adresse IP et l'évolution jurisprudentielle.

La position de la CNIL n'est pas toujours partagée par la jurisprudence française. Si dans certains arrêts elle a à juste titre prôné pour cette assimilation en affirmant que « L'adresse IP, est, au sens strict, un identifiant d'une machine lorsque celle-ci se connecte sur l'Internet et non d'une personne. Mais au même titre qu'un numéro de téléphone n'est, au sens strict, que celui d'une ligne déterminée mais pour laquelle un abonnement a été souscrit par une personne déterminée ; un numéro IP associé à un fournisseur d'accès correspond nécessairement à la connexion d'un ordinateur pour lequel une personne déterminée a souscrit un abonnement auprès de ce fournisseur d'accès. L'adresse IP de la connexion associée au fournisseur d'accès constitue un ensemble de moyens permettant de connaître le nom de l'utilisateur » [5]. Dans cet arrêt, les juges du fond se sont basés sur la définition légale de la donnée personnelle de l'article 2 de la loi du 6 janvier 1978 précitée comme étant une information qui peut identifier indirectement une personne physique par référence à un numéro d'identification.

Dans d'autres arrêts, les juges du fond français [6] ont refusé toute assimilation de l'adresse IP à une donnée personnelle [7] en ce qu'elle ne permet pas d'identifier l'auteur de la connexion [8]. Dans ce contexte, par un arrêt du 5 septembre 2007, la chambre criminelle de la Cour de cassation a considéré que l'adresse IP est une donnée parmi d'autres d'un faisceau d'indices, et donc, insuffisante à elle seule pour être qualifiée de donnée personnelle [9]

La problématique de l'adresse IP ne semble pas être résolue étant donné que cette question a été soulevée récemment devant la Cour d'appel de Rennes du 28 avril 2015, qui s'est prononcée en défaveur de cette qualification en considérant que « (...) le simple relevé d'une adresse IP aux fins de localiser un fournisseur d'accès ne constitue pas un traitement automatisé de données à caractère personnel au sens des articles 2, 9 et 25 de la loi « informatique et libertés » du 6 janvier 1978. L'adresse IP est constituée d'une série de chiffres, n'est pas une donnée, même indirectement nominative alors qu'elle ne se rapporte qu'à un ordinateur et non à l'utilisateur (...) ».

Analyse.

La problématique de cette question se résume ainsi : si l'adresse IP est considérée comme donnée personnelle cela implique qu'il s'agit d'un traitement de donnée personnelle régi par la loi du 6 janvier 1978, et de ce fait, bénéficie de l'arsenal de dispositions protectrices prévu pour protéger la personne physique d'une part, et risque de tomber sous le coup des sanctions prévues en cas de non respect des dispositions légales prévues à cet effet d'autre part.

Cela implique le recours à la CNIL en amont de tout traitement pour autorisation, et en cas de conflit, c'est le tribunal de grande instance qui sera matériellement compétent. Encore faut-il que cela concerne une personne physique dans la mesure où la loi du 6 janvier 1978 ne protège que cette catégorie de personnes.

Le seul moyen de mettre fin à cette incertitude c'est l'adoption d'une disposition légale claire et précise sur la notion de donnée personnelle. Cela pourra bientôt se concrétiser après l'adoption de la proposition de Règlement européen relatif à la protection des données à caractère personnel et sa transposition ultérieure dans le droit positif français.

Auteure : Zahra Reqba

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

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.

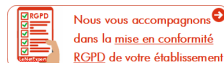
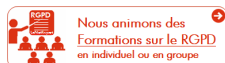


Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

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 aisé 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)

Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage



Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.

Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante :)
- Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.



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

Combien de temps une crèche peut-elle conserver des informations sur les enfants et leurs familles ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 LE NET EXPERT SPY DETECTION Services de detection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité  vous informe...		Combien de temps une crèche peut-elle conserver des informations sur les enfants et leurs familles ?			
Les crèches et les autres structures d'accueil de jeunes enfants sont amenées à enregistrer dans leur logiciel de gestion des informations personnelles sur les enfants accueillis et sur leurs parents. La durée de conservation de ces informations ne doit pas dépasser la durée nécessaire aux finalités pour lesquelles ces informations sont collectées et traitées. Dans le cas de l'accueil de jeunes enfants, la CNIL recommande que ces informations soient effacées au plus tard trois ans après leur départ. Au-delà de ce délai, elles ne peuvent être conservées que de manière anonymisée, dans un but statistique par exemple.					

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.



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

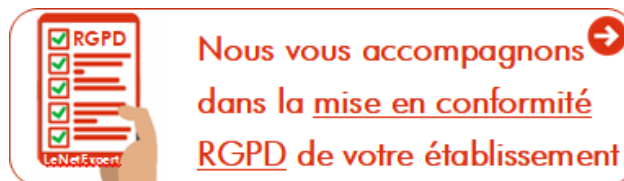
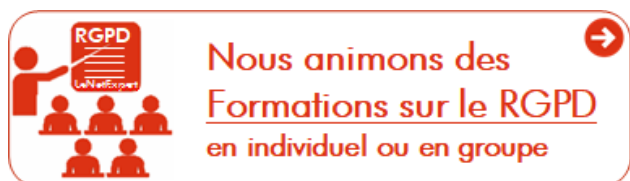
Contactez-nous

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 aisé 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 :
<http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=193E337DAA685A15B25C9E90E19E80BF?name=Combien+de+temps+une+cr%C3%A8che+peut-elle+conserver+des+informations+sur+les+enfants+et+leurs+familles+%3F&id=483>

Mettre son établissement en conformité avec la CNIL, mode d'emploi | Denis JACOPINI



Mettre son établissement en conformité avec la CNIL, mode d'emploi

Se mettre en conformité avec la CNIL est une obligation depuis 1978.

Cependant, les préoccupations des établissements et organismes étant principalement orientées vers des réglementations sociales, fiscales et celles liées à leur métier, la réglementation numérique est longtemps restée délaissée.

En rapport direct avec l'explosion de la cybercriminalité en France, le non respect de la Loi Informatique et Libertés est de plus en plus montré du doigt et les établissements piratés ont de plus en plus leur image salie et leurs comptes bancaires siphonnés.

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.

UNE MISE EN CONFORMITÉ CNIL DOIT PASSER PAR UN AUDIT DE L'ENSEMBLE DE VOS SYSTÈMES DE TRAITEMENTS DE DONNÉES

Que se cache derrière cette loi ?

Quels sont les étapes indispensables et les pièges à éviter pour que cette mise en conformité ne se transforme pas en fausse déclaration ?

Plus d'information sur : www.cnil.lenetexpert.fr

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

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.aide.cnil.fr/selfcnil/site/template.do?id=572&back=true>

RGPD Règlement européen sur la protection des données : ce qui change pour les professionnels



RGPD Règlement européen sur la protection des données : ce qui change pour les professionnels

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

- Un cadre juridique unifié pour l'ensemble de l'UE
- Un renforcement des droits des personnes
- Une conformité basée sur la transparence et la responsabilisation
- Des responsabilités partagées et précisées
- Le cadre des transferts hors de l'Union mis à jour
- Des sanctions encadrées, graduées et renforcées
- Comment les autorités de protection se préparent-elles ?

Où trouver le texte officiel du RGPD (Règlement européen sur la protection des données) ?

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 RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Réagissez à cet article

Source : *Règlement européen sur la protection des données :
que faut-il savoir ? | Besoin d'aide | CNIL*