

Formation Data protection officer (DPO)

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Formation Data protection officer (DPO)

Le data protection officer sera obligatoire en France dans certaines entreprises le 25 mai 2018. Voici ce qu'il faut savoir sur son rôle.

D'ici le 25 mai 2018, les entreprises et les administrations qui utilisent des données à caractère personnel devront recourir aux services d'un data protection officer (DPO).

Quel est son rôle et ses obligations ?

Data protection officer : définition

Les données sont présentes en masse dans les entreprises. Ce qui peut poser des risques en matière de sécurité mais aussi de légalité. Pour aider les entreprises, un nouveau métier a le vent en poupe dans le secteur du numérique : le data protection officer (DPO).

Sa mission est la suivante : s'assurer que son employeur ou son client respecte la législation lorsqu'il utilise les données à des fins commerciales (mailing par exemple) mais aussi à des fins internes (logiciels RH). Son rôle est donc transversal, ce qui l'amène à travailler avec de nombreux départements : direction générale, marketing, développement ou encore RH. En cas de manquement à la loi, il est tenu d'alerter sa direction dans les plus brefs délais.

Son rôle est très polyvalent. En plus de connaissances en informatique et en cybersécurité, le data protection officer est tenu de posséder une grosse culture juridique, notamment en droit des nouvelles technologies de l'information et de la communication (NTIC). Aujourd'hui, des juristes spécialistes des NTIC, des informaticiens, des ingénieurs en cybersécurité peuvent exercer des fonctions de data protection officer au sein d'entreprises ou de cabinets de conseil.

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)

Réagissez à cet article

Source : *Data protection officer (DPO) : définition, formation et salaire*

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

x

x

x

x

x

x

x

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Il n'est pas possible pour l'employeur d'utiliser les résultats de la géolocalisation si ce n'est pas déclaré à la CNIL (Commission nationale de l'informatique et des libertés) et sans que le sache le salarié, encore moins si l'entreprise possède déjà un moyen de contrôler la durée de travail. Si un salarié a une liberté de son temps de travail, c'est surtout le résultat qui compte.

Réagissez à cet article

Quelques articles sélectionnés par nos Experts :

[Quels sont les droits et devoirs des salariés en matière de sécurité informatique](#)

[La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?](#)

[Accompagnement à la mise en conformité avec le RGPD de votre établissement](#)

[Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?](#)

[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)

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



Notre Expert, Denis JACOPINI est Expert de justice en
informatique spécialisé en cybercriminalité et en protection
des Données à Caractère Personnel, formateur depuis 1998 et

consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*

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

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

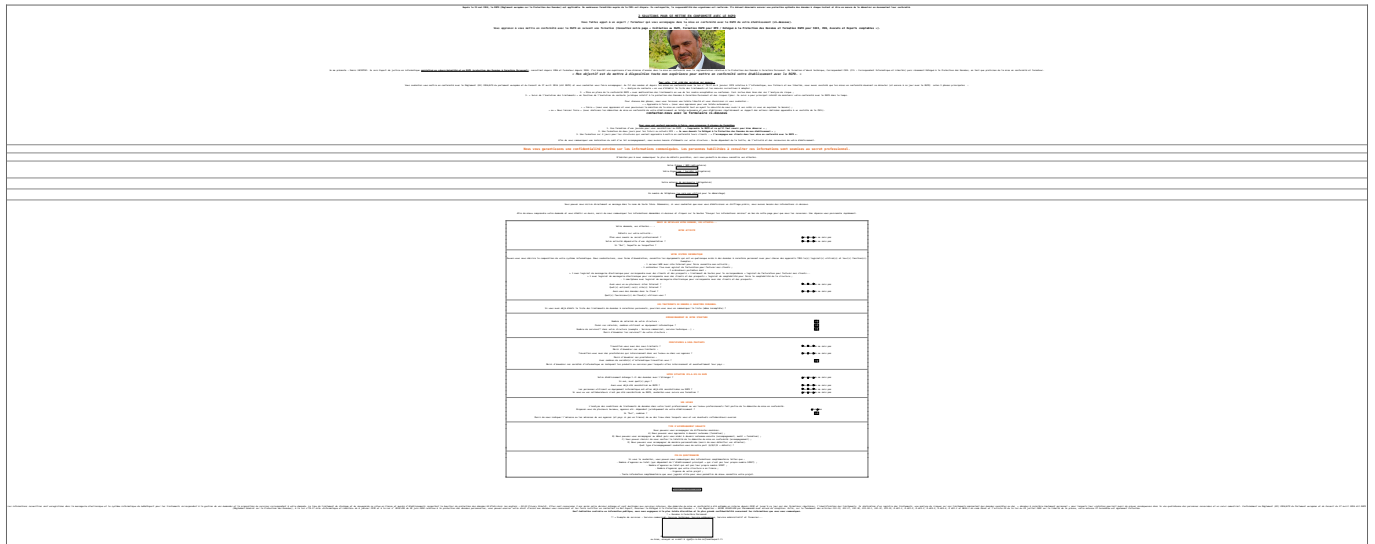


Depuis 2012, nous accompagnons des

établissement dans leur mise en conformité avec la réglementation sur les Données à Caractère Personnel.



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



Source : Denis JACOPINI

Le dirigeant est responsable de ses déclarations à la CNIL | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Le dirigeant est responsable de ses #déclarations à la CNIL

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations [ici](https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd) : <https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd> Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations ici : <https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd> Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

Quelles mesures les entreprises doivent-elles prendre pour être en règle avec la CNIL (commission nationale de l'informatique et des libertés), notamment pour le respect des données privées ?

Les entreprises doivent protéger les données personnelles, selon la loi Informatique et libertés ?

C'est une obligation légale des entreprises : elles doivent protéger les données personnelles de leurs salariés comme de leurs clients. Une donnée personnelle est toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement .

Certaines données peuvent sembler évidentes : nom, prénom, date de naissance, adresse postale, empreinte digitale. D'autres viennent moins spontanément à l'esprit : adresse IP, habitudes de consommation, entourage familial, plaque d'immatriculation.

L'entreprise se doit donc de sécuriser les informations personnelles qui transitent par son site Internet (ne serait-ce qu'à travers un formulaire de contact), par l'enregistrement des appels, la vidéosurveillance, l'annuaire interne, les contrôles d'accès aux locaux, etc.

Que doit faire l'entreprise pour être en conformité avec la loi ?

Informers les instances représentatives et mettre en œuvre une charte informatique ne suffit pas. Le site Internet de l'entreprise doit comporter des mentions légales, elle doit assurer la confidentialité des données, définir une durée de conservation des données, effectuer les déclarations préalables à la mise en place d'un dispositif de collecte auprès de la CNIL, respecter l'objectif de la collecte annoncé, etc.

Le dirigeant de l'entreprise est responsable et doit prendre les mesures nécessaires au traitement des données personnelles. Il est aussi fortement conseillé, dans les entreprises de taille importante, de mettre en place un CIL, un correspondant informatique et libertés, et de sensibiliser les utilisateurs et les salariés aux risques informatiques et à la loi informatique et libertés. Il peut aussi être utile de faire un inventaire des traitements des données à caractère personnel (site Internet, fichiers clients, prospects, fournisseurs, téléphonie, vidéo-surveillance, gestion de la paie, fichiers métiers).

Le coût de la mise en place de ces mesures varie en fonction de la taille de l'entreprise, donc du temps nécessaire à l'analyse des risques.

Quelles sanctions l'entreprise et son dirigeant risquent-ils ?

Au-delà des sanctions légales, c'est la réputation et la crédibilité de l'entreprise qui sont en jeu : son image et son patrimoine sont exposés.

Néanmoins, l'absence de mentions légales peut déboucher sur une amende de 6000 €, la surveillance permanente des zones réservées dans une entreprise ou la collecte de données sur la vitesse d'un véhicule, 5000 € ; le non respect des obligations de sécurisation des données personnelles peut aller jusqu'à 300 000 € d'amendes. □ Toutefois, la CNIL joue pour l'instant avant tout un rôle de prévention plus que de sanction.

Quid de la loi sur le renseignement qui oblige les opérateurs à mettre en place des dispositifs automatiques de collecte des données ?

Ce type de loi ne pose pas de problème dans une démocratie et remplit ses objectifs de sécurité. En revanche, la question se poserait de façon plus grave sous un autre régime.

ATTENTION !

Nous attirons votre attention particulièrement sur le fait que certains professionnels du monde informatique, de l'internet ou de la communication, concernés par un devoir d'information auprès de leurs clients, remplissent les déclarations à la CNIL de leurs clients pour leur simplifier les démarches.

Il faut savoir que la déclaration à la CNIL d'un système de traitement se compose d'abord d'un audit technique et logique de l'existant, tant au niveau organisationnel qu'au niveau technique jusqu'à la sécurité informatique mise en place.

Une déclaration incomplète ou ne correspondant pas à la réalité peut vite se transformer en FAUSSE DECLARATION.

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)

Réagissez à cet article

Source :
<http://www.tracescritesnews.fr/actualite/le-dirigeant-est-responsable-de-la-securite-informatique-de-l-entreprise-et-des-donnees-personnelles-56747>
par Pierre-Yves Ratti

Prospection par messagerie électronique : que risque une société qui ne respecte pas la loi ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



#Prospection par
messagerie électronique
que risque une société qui
ne respecte pas la loi ?

Une société commerciale ne peut envoyer de mails publicitaires sans l'accord préalable de la personne sollicitée.

Une société qui ne respecte pas cette règle risque des sanctions pénales et des amendes de 750 euros par message expédié.

De son côté, la CNIL peut prononcer des sanctions pouvant aller jusqu'à 300.000 Euros d'amende lorsque des messages sont adressés à des personnes physiques sans leur consentement.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD) et à se protéger des pirates informatiques.**

Quel sont nos principales activités ?

- **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)





Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

*« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »*

Besoin d'un Expert ? contactez-nous

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](#)



Source : <https://www.cnil.fr/fr/cnil-direct/question/372>

Quels sont les droits et devoirs des salariés en matière de sécurité informatique | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Quels sont les droits et devoirs des salariés, en matière de sécurité informatique				

Il n'est pas rare que des salariés soient surpris en train, au sein de leur entreprise, d'utiliser des outils de type Keylogger – permettant l'enregistrement des touches utilisées sur le clavier – et des logiciels visant à capter et à forcer les mots de passe de sessions de systèmes d'exploitation.

Or, dans la majorité des cas, aucune sanction n'est prise par les employeurs, y compris lorsque les auteurs des faits sont animés d'intentions malveillantes et non simplement ludiques.

Dans un raisonnement inspiré du droit du travail, l'employeur – arguant par exemple de ne pas disposer de charte de sécurité informatique spécifiant les comportements à respecter, ainsi que les sanctions applicables – estime qu'à défaut d'avoir porté par écrit à la connaissance de l'employé la réglementation en vigueur au sein de l'entreprise, celui-ci ne peut être légalement sanctionné.

Il est important de rappeler que le seul fait de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code pénal) et ce, quelles que soient les intentions du salarié. De même, le fait de s'introduire frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d'amende (article 321-1 du même code). La loi est d'application directe et ne nécessite pas d'être citée dans une charte informatique pour en assurer le respect par les salariés. Les employeurs peuvent donc prendre immédiatement les sanctions afférentes à une telle faute.

En outre, la responsabilité de l'employeur peut se voir engagée par ce type d'agissements, sur la base de plusieurs fondements :

- la personne cible/victime des menées de son/ses collègues pourra, en cas de dommage, agir contre l'employeur, responsable de ses salariés. Il reviendra alors à la société de prouver que le mis en cause a agi « hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions », ce qui est rarement admis en pratique.
- de par la jurisprudence « Sarenza c/ Jonathan » du 21 février 2013, le juge a précisé que la société devait supporter, à hauteur de 30%, son propre dommage, engendré par les lacunes dans la gestion des identifiants d'accès aux bases de données. Le juge a donc instauré l'obligation, pour l'employeur, de mettre en place des mesures de protection informatique efficaces, afin de prévenir l'installation de tout logiciel espion.
- Enfin, la plupart des logiciels utilisés à ces fins proviennent de téléchargements, susceptibles de contenir des virus. Les réseaux internes des entreprises sont régulièrement infectés par ce biais, ce qui facilite les intrusions informatiques et, partant, l'accès, l'utilisation, l'extraction, voire la destruction de données stratégiques pour l'entreprise.

Préconisations de la DGSJ

La DGSJ recommande à toute entreprise :

- En priorité, d'établir une charte de sécurité informatique qui permettra de sensibiliser les salariés aux enjeux numériques, tout en les responsabilisant.
- D'organiser régulièrement des conférences de sensibilisation à destination de l'ensemble des collaborateurs, qui insisteront sur leurs droits et obligations à l'ère du tout-numérique et dispenseront des mises à jour sur les évolutions technologiques en cours.
- De mettre en place des mesures de protection efficaces afin de prévenir l'utilisation potentielle de logiciels et matériels espions. L'existence de tels dispositifs de sécurité informatique permettra à l'employeur de dégager sa responsabilité juridique et d'optimiser le bon fonctionnement de son entreprise en augmentant le niveau de protection.

Vous avez besoin de recueillir des preuves, expertiser un système informatique, vérifier des contenus, Denis JACOPINI peut vous conseiller, vous accompagner et réaliser toutes les phases techniques nécessaires à la constitution d'un dossier juridique solide.

Contactez Denis JACOPINI

Réagissez à cet article

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

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



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».

Source

<http://www.ccirezo-normandie.fr/document/104108-flash-ingerence-economique-n-15-rappel-des-droits-et-devoirs-des-salaries-en-entrepr>

Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

2 SOLUTIONS POUR SE METTRE EN CONFORMITÉ AVEC LE RGPD

Vous apprenez à vous mettre en conformité avec le RGPD en suivant une formation (ci-dessous) ;

Vous faites appel à un expert / formateur qui vous accompagne dans votre mise en conformité avec le RGPD de votre établissement (Consultez notre page « Services d'accompagnement à la mise en conformité avec le RGPD »).



Je me présente : Denis JACOPINI. Je suis Expert de Justice en informatique spécialisé en cybersécurité et en RGPD (protection des données à caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il est ainsi aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Pour cela, j'ai créé 3 niveaux de formation.

1. Une formation d'une journée pour les indépendants, TPE et les PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer ». Cette formation a pour objectif de vous faire découvrir l'essentiel de ce règlement Européen, de vous apprendre les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions ;
2. Une formation de deux jours pour les DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement ». Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement ;
3. Une formation sur 4 jours pour les consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD ». Vous êtes une société d'informatique, un cabinet d'avocat, un cabinet d'expertise comptable et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation est composée de 2 jours de théorie et 2 jours de pratique dont 1 dans l'établissement de votre choix (le votre ou celui d'un client). Suivez la formation qui vous apportera la plus grande autonomie avec le RGPD de tout notre catalogue.

et des services sur mesure.

1. Vous souhaitez tout faire -> Nous vous apprendrons à mettre votre établissement en conformité, la plupart du temps, le contenu de ces formations est personnalisé et adapté à vos besoins spécifiques ;
2. Vous ne savez pas par où commencer -> Nous ferons l'état des lieux, mettrons en place le registre puis nous vous apprendrons à maintenir la conformité des traitements ;
3. Vous ne souhaitez rien faire -> Nous nous occuperons de tout.

Plus d'information sur nos services d'accompagnement à la mise en conformité avec le RGPD ici

Formation pour TPE/PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer » : 1 jour

Découvrez l'essentiel du RGPD, apprenez les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions.
Consultez les dates de nos prochaines formations
« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours

(Découvrez et comprenez la démarche de mise en conformité)
Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement.
Consultez les dates de nos prochaines formations
« Je veux devenir le Délégué à la Protection des Données de mon établissement »

Formation pour consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour dans votre établissement

(C'est le moment où jamais de vendre des services autour du RGPD)
Enfin, si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de vendre cette prestation auprès de vos clients, cette formation est faite sur mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en conformité. Vous êtes une société d'informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez la formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue.
Consultez les dates de nos prochaines formations
« J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Formation RGPD « Mise en conformité RGPD sur mesure » (pour TPE/PME)

(Pour ceux qui souhaitent une formation ou un accompagnement personnalisé dans la mise en conformité RGPD)

Que vous soyez bientôt ou déjà désigné « Délégué à la Protection des Données » ou « DPO » dans votre établissement, si vous souhaitez que nous établissions une formation personnalisée dans son contenu ou dans son organisation, nous nous ferons un plaisir d'étudier votre demande et d'élaborer une proposition adaptée à vos besoins.

Accompagnement à la mise en conformité RGPD de mon établissement

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des données à caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » ;
- ou « Nous laisser faire ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

N'hésitez pas à contacter notre équipe.

Intéressé pour assister à une de nos sessions de formation en France, choisissez la ville qui vous intéresse. Vous souhaitez que nous nous déplaçons au sein de votre établissement pour une formation ou pour un accompagnement individuel, indiquez le dans les commentaires.

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :

- la formation « Comprendre le RGPD » : 1 jour
- la formation « Je veux devenir Délégué à la Protection des Données » : 2 jours
- la formation « Je mets en conformité mon établissement » : 3+1 jours
- la formation « Mise en conformité RGPD sur mesure »
- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs places à la formation :

Formation pour TPE/PME : « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : « Je veux devenir le Délégué à la Protection des Données de mon établissement »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : « J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre accepté. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre accepté sera remboursé en intégralité dans les 5 jours (Les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'accepté pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

LE FORMATEUR : Denis JACOPINI



Denis JACOPINI est Expert de Justice en informatique spécialisé en cybersécurité et en RGPD (protection des données à caractère Personnel). Il est diplômé en Cybersécurité, et, titulaire de l'expertise Judiciaire et est Certifié en Gestion des Risques des Systèmes d'Information. Il est formateur depuis 1998 et consultant depuis 1996, il a 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 dans la sécurité informatique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il est ainsi aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD à tout public.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

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)

Réagissez à cet article

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

Les grands principes de la cryptologie et du chiffrement

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Les grands principes de la cryptologie et du chiffrement				

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage. À l'occasion du mois européen de la cybersécurité, la CNIL vous explique ce que c'est et à quoi ça sert.

Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός). Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).

La cryptologie ne se limite plus aujourd'hui à assurer la confidentialité des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'authenticité d'un message (qui a envoyé ce message ?) ou encore assurer son intégrité (est-ce qu'il a été modifié ?).

Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.

Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.

Pour découvrir les grandes phases de l'histoire de la cryptologie, rendez-vous sur le webdocumentaire réalisé par l'ANSSI.

Pourquoi la cryptologie existe-t-elle ?

1.

Pour assurer l'intégrité du message : le hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « fonction de hachage » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2 » ou « SHA256 ».

Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès (voir « Pour assurer la confidentialité du message »), et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.

Le hachage, pour quoi faire ?

Pour sauvegarder vos photos sur votre espace d'hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s'est bien déroulé ?

Pour synchroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés ?

Il existe aussi des « fonctions de hachage à clé » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.

Le hachage à clé, pour quoi faire ?

Votre service préféré reconnaît votre mot de passe quand vous vous connectez ?

Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire ?

2.

Pour assurer l'authenticité du message : la signature

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « signature » – numérique – permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

La signature numérique, pour quoi faire ?

Vous voulez garantir être l'émetteur d'un courriel ?

Vous voulez vous assurer qu'une information provient d'une source sûre ?

Pour pouvoir signer, Alice doit se munir d'une paire de clés :

- l'une, dite « publique », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu'envoie Alice ;
- l'autre, dite « privée », qui ne doit être connue que d'Alice.

En pratique, Alice génère sa signature avec sa clé privée qui n'est connue que d'elle. N'importe quelle personne ayant accès à la clé publique d'Alice, dont Bob, peut vérifier la signature sans échanger de secret.

3.

Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d'un message permet justement de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

Le chiffrement, pour quoi faire ?

Vous voulez vous assurer que seul le destinataire ait accès au message ?

Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?

Il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Le **chiffrement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.

Le **chiffrement asymétrique** suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire.

Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s'en dispenser. Mais il est malheureusement plus lent.

Pour cette dernière raison, il existe une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « **chiffrement hybride** ».

Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque vous visitez un site dont l'adresse débute par « https ».

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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](#)



Source

<https://www.cnit.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>

Le livre du jour : CYBERARNAQUES – a l'écoute des livres, Radio Massabielle (97.8 Mhz et 101.8 Mhz)

Notre métier en RGPD et en CYBER : Auditer, Expertiser,
Accompagner, Former et Informer



Le livre du jour :
CYBERARNAQUES – a l'écoute
des livres, Radio
Massabielle (97.8 Mhz et
101.8 Mhz)

Comme les langues d'Esopé, Internet peu être la meilleure et la pire des choses. En effet s'il permet de relier les femmes et les hommes à travers le monde, de travailler, de s'informer, etc.. il es également le point de toutes sortes d'escrocs. Aussi, en répondant à une annonce ou au message que vous pensez être envoyé par un ami, vous risquez de voir votre compte en banque vidé ou d'être victime d'un chantage. Les CYBERARNAQUES sont légion et il convient de s'informer pour mieux protéger votre famille et vos biens. Combien d'entre-nous n'on pas vérifié...[lire la suite]

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)

Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la

Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur [Fnac.fr](https://www.fnac.fr)

Source : *Le livre du jour : CYBERARNAQUES – à l'écoute des livres*

**Protection des données
personnelles : Les
entreprises ne respectent pas
la Loi et jouent avec les
données de leur clients. Ça
pourrait bien leur coûter
cher ! | Denis JACOPINI**

Notre métier en RGPD et en CYBER : Auditer, Expertiser,
Accompagner, Former et Informer





Protection des
données
personnelles.
: Les entreprises
ne respectent pas
la Loi et jouent
avec les données
de leur clients.
Ca pourrait bien
leur coûter cher
!

Depuis 1978, les entreprises sont soumises à des obligations en terme de déclaration de traitements de données personnelles à la CNIL. Ne pas se soumettre à ces obligations, rend pénalement responsable le chef d'entreprise et passible d'une amende jusqu'à 300 000 euros. Une loi et des obligations quasiment tout le temps oubliées. Depuis le 25 mai 2018, les sanctions sont portées à 20 millions d'euros ou 4% du chiffre d'affaire.

A quoi sert la CNIL ?

Positionnez-vous d'abord en tant que consommateur. Lorsque vous commandez, achetez, communiquez, savez-vous où vont les informations personnelles ou confidentielles que vous confiez aveuglément ? Seriez-vous d'accord si toutes les données (coordonnées postales, e-mail, bancaires, santé, politique, religion, habitudes de consommation etc.) que vous communiquez en toute confiance à des tiers se retrouvent dispersées dans la nature et à la vue de tout le monde ? J'imagine que non ! Vous vous attendez plutôt à ce que tous les tiers prennent soin de conserver précieusement vos informations qui sont pour chacun d'entre nous précieuses et confidentielles pour certaines.

A la place de ça, que font les entreprises ?

Ils utilisent vos coordonnées pour envoyer de la publicité et surcharger votre boîte e-mail, votre téléphone, votre boîte aux lettres. Plus grave, certains vont vendre ou louer vos coordonnées à des tiers pour monnayer vos informations personnelles. Plus grave encore, d'autre encore vont stocker vos précieux éléments sur des systèmes informatiques non sécurisés... Et c'est aussi comme ça qu'on se retrouve rapidement noyé par les spams ou les virus, victime d'usurpation d'identité ou pire... C'est pour canaliser cela que la CNIL (Commission Nationale de l'Informatique et des Libertés) existe. Sa mission officielle est de « veiller à ce que le développement des nouvelles technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Qui est concerné ?

Tout professionnel, organisme, association qui gère un fichier client, contact, mail, salariés, élèves, patients... que ce fichier soit informatisé ou géré sur papier. Les seuls qui n'ont pas à faire de telles déclarations sont les particuliers et les associations, mais seulement pour les traitements qui concernent les données de leurs membres.

Les réactions les plus courantes lors de mes conférences

Lorsqu'il anime des ateliers, des tables rondes ou des conférences sur le sujet des risques juridiques du chef d'entreprise face aux nouveaux usages de l'informatique ou des obligations des entreprises vis à vis de la CNIL, et que le volet des obligations par rapport à la loi Informatique et Libertés est abordé, il m'est systématiquement posé la question suivante :

« Mais, comment se fait-il qu'on ne soit pas informé de ces obligations ? »

Et ma réponse au chef d'entreprises est systématiquement toujours la même :

« Par pure négligence de votre part... Que votre entreprise ait 0 ou 100 000 salariés, les obligations sont les mêmes et existent depuis 1978 au travers de la Loi Informatique et Libertés. Lorsque vous avez créé votre entreprise, vous vous êtes engagés à respecter la réglementation pendant toute la vie de votre entreprise. Et cette loi, je vous l'accorde, longtemps restée dans l'ombre, fait partie des règles qui doivent être obligatoirement respectées. Comme vous avez vu tout à l'heure, si vous vous positionnez en tant que consommateur, il vous semble évident que vos données personnelles soient protégées. Comme cette précaution absolue n'est pas une priorité naturelle pour les entreprises, un gendarme a été créé pour informer, surveiller, contrôler et sanctionner les entreprises fautives. Vous faites certainement partie des patrons qui essaient de gérer leur entreprise du mieux possible et avec vos problèmes et avec vos priorités vous y arrivez je pense très bien. Vous vous souciez probablement d'abord de la réglementation à respecter en matière sociale, fiscale et en rapport de votre activité professionnelle. Je sais qu'il est matériellement impossible de tout savoir, et de connaître toutes les lois. C'est ce que moi j'appelle faire des impasses. Sauf que là, c'est des impasses qui peuvent vous coûter jusqu'à 300 000 euros. »

Pourquoi parle-t-on de la CNIL si souvent aujourd'hui ?

Parce qu'elle tire la sonnette d'alarme devant les changements de nos habitudes et l'évolution de la technologie fait très important qui s'est passé depuis le début des années 80 : L'informatique s'est répandue dans quasiment tous les domaines sans réellement tenir compte de la sécurité des données. Peu savent que depuis les années 90, Internet qui s'impose à nous utilise un protocole de communication qui à la base ne sont pas sécurisés... Ensuite, nous sommes entrés dans l'ère des objets connectés avec un risque permanent de se faire « pomper » nos données. On ne va plus seulement parler de coordonnées postales téléphoniques ou bancaires, mais aussi de données de santé, d'habitudes alimentaires, de sommeil, de sortie, de loisirs... Que vos joujoux hi-tech connectés, votre smartphone ou votre ordinateur soient perdus ou piratés, les données qu'ils stockent sont librement accessibles. De plus, il ne se passe pas un jour sans qu'un opérateur, une société Web, une entreprise se fasse pirater son système informatique et par la même occasion les données de ses clients. Il y a deux types de cibles : celles qui ont beaucoup de trésorerie à se faire voler, et les millions de malchanceux qui dont le manque de sécurité a été automatiquement détecté qui vont être la proie de cybercriminels. Pour vous donner une idée, 144 milliards d'emails sont échangés chaque jour et 68,8% d'entre eux sont des spams et nombreux cachent des réseaux cybercriminels. 400 Millions de personnes sont concernées par des cyberattaques chaque année. Vous comprenez maintenant pourquoi il devient urgent de canaliser tous ces usages et déjà les premiers débordements avant que ça continue à s'aggraver.

Est-ce risqué de ne pas respecter la Loi Informatique et Libertés

Même si en référence la loi du 29 mars 2011 relative au défenseur des droits, la CNIL peut rendre publiques les sanctions pécuniaires qu'elle prononce, il n'y a jusqu'à maintenant eut que très peu de sanctions prononcées. En 2013, 414 contrôles ont abouti à 14 sanctions.

On eut en avoir liste sur <http://www.cnil.fr/institution/missions/sanctionner/les-sanctions-prononcees-par-la-cnil/> Cependant, le niveau de risque devrait exploser en 2015 ou du moins, dès la mise en application du règlement européen relatif aux traitements de données à caractère personnel. Selon les infractions, le montant des sanctions peut aujourd'hui s'élever jusqu'à 300 000 euros. Cependant, compte tenu de leur chiffre d'affaire démesuré, certaines entreprises peuvent continuer à sourire avec de telles amendes (par exemple google et ses 60 milliards de chiffre d'affaire, ou Facebook, Appel, Orange) .

Devant ces situations, la Commission Européenne décide de frapper un grand coup avec un règlement européen et au travers de deux principales actions réglementaires :

- 1) Augmenter plafonds des amendes jusqu'à 5% du chiffre d'affaire (ça pourrait donner 3 milliards de dollars d'amende maximale par infractions pour google)
- 2) Rendre Obligatoire pour toute entreprise, de déclarer sous 24h à la CNIL le moindre incident de sécurité (virus, perte données, perte ou vol de matériel, piratage...), laquelle pourra vous obliger d'informer tous vos clients que la sécurité de leurs données personnelles a été compromise. Cette obligation existe déjà depuis juin 2013 mais seulement pour les OIV (Opérateurs d'importance Vitale).
- 3) Souvenez-vous l'affaire du piratage d'Orange en janvier et avril 2014 et les articles de presse peu valorisants pour la marque et inquiétant pour ses clients. Le règlement européen prévoit d'obliger toutes les entreprises d'informer l'ensemble des propriétaires dont la sécurité a été compromise suite à un piratage, une perte ou à un vol de données personnelles ou de matériel contenant des données personnelles. Ainsi, on ne parle plus d'un risque financier, mais d'un risque de mauvaise réputation des entreprises face à leurs clients et concurrents.

Concrètement, que faut-il faire pour se mettre en conformité avec la CNIL ?

L'article premier de la Loi définit que l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

L'article 2 précise que la loi s'applique aux traitements de données à caractère personnel contenues ou appelées à figurer dans des fichiers.

Enfin l'article 22 indique que les traitements de données à caractère personnel font l'objet d'une déclaration auprès de la CNIL.

En d'autres termes, pour se mettre en conformité, il faut déclarer à la CNIL l'ensemble des traitements de données qui concernent des informations permettant d'identifier des personnes.

Je tiens à préciser qu'on ne déclare pas ou on ne donne pas à la CNIL ses données, on ne déclare que des traitements de données à caractères personnel.

Lien vers la Loi Informatique et Libertés <http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/>

Mon conseil en 4 étapes pour se mettre en conformité avec la CNIL

- 1) Identifier l'ensemble des traitements de données permettant d'identifier des personnes.
 - 2) Procéder à l'analyse détaillée de ses traitements et corriger les actions qui ne sont pas conformes à la Loi Informatique et Libertés en terme de sécurité des fichiers, de confidentialité des données, de durée de conservation des documents, d'information des personnes, de demande d'autorisation et de finalité des traitements.
 - 3) Déclarer le traitement à la CNIL ou désigner un Correspondant Informatique et Libertés qui sera chargé de tenir à jour un registre des traitements sans avoir à les déclarer séparément.
 - 4) Faire un à deux points par an pour reporter dans le registre les changements sur les traitements existants et les y ajouter les nouveaux.
- En cas d'impossibilité d'adapter votre traitement de données personnelles par rapport à la loi Informatique et Libertés, une demande d'avis ou d'autorisation doit être formulée à la CNIL.
- Bien évidemment, la réponse de la CNIL doit être attendue avant d'utiliser le traitement concerné.
- Une fois ces étapes de « mise sur rails » accomplie, la personne qui aura en charge la fonction de correspondant dans votre entreprise aura obligation de tenir un registre des traitements mis en œuvre au sein de l'organisme (consultable par la CNIL ou tout demandeur sur simple demande) et de veiller au respect des dispositions de la loi « informatique et libertés » au sein de l'organisme.

Est-on obligé de faire une déclaration pour chaque traitement ?

Oui et Non
Non si vous nommez un Correspondant Informatique et Libertés (CIL). Ou'il soit interne à l'entreprise ou externe (si vous souhaitez déléguer la responsabilité à quelqu'un d'externe à l'entreprise, comme je le fais pour de nombreuses entreprises). Le CIL n'aura alors qu'à tenir à jour un registre répertoriant l'ensemble des traitements de données à caractères personnel et leurs caractéristiques détaillées. Ce registre devra pouvoir être consultable par la CNIL mais aussi par quiconque vous en fera la demande.
Oui si vous décidez de ne pas déclarer un Correspondant Informatique et Libertés.

Qui peut être ou devenir CIL ?

La loi prévoit que le correspondant Informatique et Libertés est une personne bénéficiant des qualifications requises pour exercer ses missions.

Aucun agrément n'est prévu et aucune exigence de diplôme n'est fixée.

Néanmoins, le CIL doit disposer de compétences variées et adaptées à la taille comme à l'activité du responsable des traitements.

Ces compétences doivent porter tant sur l'informatique et les nouvelles technologies que sur la réglementation et législation relative à la protection des données à caractère personnel.

-
L'absence de conflit d'intérêts avec d'autres fonctions ou activités exercées parallèlement est également de nature à apporter les garanties de l'indépendance du CIL. C'est pourquoi la fonction de correspondant est incompatible avec celle de responsable de traitements. Sont concernés le représentant légal de l'organisme (ex. : le maire / le PDG) et les autres personnes participant à la prise de décisions en matière de mise en œuvre des traitements (ex. : les conseillers municipaux / les personnes disposant d'une délégation de pouvoirs).

Des difficultés pour vous mettre en conformité ?

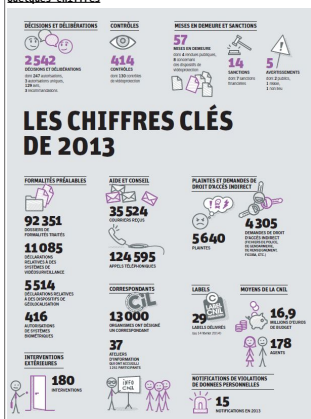
Pour vous mettre en conformité avec la CNIL, il vaut mieux être sensibilisé à la loi Informatique et Libertés et aux règles et obligations qui en découlent (obligation d'information, droit d'accès, traitement des réclamations...).

Pour que votre mise en règle se fasse dans de bonnes conditions, nous pouvons nous charger de former et de suivre une personne de votre entreprise qui jouera le rôle de CIL (Correspondant Informatique et Libertés) ou bien, si vous le préférez, pour encore plus de tranquillité, Denis JACOPINI, expert Informatique spécialisé en protection des données personnelles, peut se charger d'être votre CIL externe en se chargeant de prendre en charge l'ensemble des formalités.

Plus de détails sur la CNIL

La CNIL est une AAI (Autorité Administrative Indépendante). C'est une structure gérée par l'état qui ne dépend d'aucun ministère et qui peut dresser des procès verbaux et sanctionner sans même à avoir à passer par un juge. La CNIL dépend directement du premier ministre qui peut en dernier recours, directement prendre des mesures pour mettre fin aux manquements.

Quelques chiffres



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)

Réagissez à cet article

Auteur : Denis JACOPINI