

6 bonnes pratiques pour se protéger du piratage informatique



6 bonnes
pratiques
pour se
protéger du
piratage
informatique

Par manque de temps ou de ressources, les PME négligent le risque de piratage informatique. Quelques règles de bon sens suffisent pourtant à écarter en partie les menaces.

Perdre ses données suite à une attaque informatique peut avoir de lourdes conséquences pour une start-up ou une PME. L'entreprise peut même ne jamais s'en relever. Piratage de site Internet, clé USB piégée, vol de mot de passe, programme espion caché dans des pièces jointes... Les cyber menaces sont de plus en plus fréquentes. Quelles sont les règles simples pour s'en protéger ? Le point avec Stéphane Dahan, président de Securiview, entreprise spécialisée dans le management de la sécurité informatique.

#1 : Identifier les données les plus sensibles

« Faites preuve d'une saine paranoïa, affirme Stéphane Dahan. C'est-à-dire sachez définir précisément quelles sont les informations à protéger dans l'entreprise ». Inutile donc de mettre des barrières partout sans discernement. Quelle que soit leur forme (mail, papier, fichier), posez vous donc la question : quelles sont les données les plus sensibles et quelle est la probabilité qu'on me les vole ? « Ensuite, il faut les localiser. Messagerie, Dropbox, téléphone, autant de pistes de fuite possible pour des informations qui ont de la valeur. »

#2 : Mettre à jour les systèmes et sauvegarder

« Ne pas oubliez de mettre à jour régulièrement ses antivirus et ses systèmes d'information. On voit trop souvent des entreprises négliger cet aspect », soutient Stéphane Dahan. N'oubliez pas non plus de **sauvegarder périodiquement vos dossiers stratégiques**. « Idéalement, ils doivent être stockés à plusieurs endroits. Si un serveur brûle, que vous soyez capable de les retrouver ailleurs ».

#3 : Assurer la confidentialité des données clés

A l'intérieur de l'entreprise, assurez-vous que seuls les salariés ayant besoin des informations sensibles puissent y accéder. Par exemple, que les mots de passe ou clés de chiffrement ne soient **attribués qu'aux personnes qui ont besoin de les connaître**.

#4 : Définir et faire appliquer la politique de mot de passe

Attention dans le choix des mots de passe ! C'est trop souvent le talon d'Achille des systèmes d'information. « Éviter de choisir les plus bateau comme abc123 ou 12345, une mauvaise habitude plus courante qu'on ne le dit », insiste Stéphane Dahan. Idéalement, fixez des règles de choix et de dimensionnement des mots de passe et **renouveler ces derniers régulièrement**.

#5 : Protéger les terminaux mobiles

Les postes mobiles sont des points d'accès potentiels pour des pirates informatiques. Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information), ils doivent bénéficier au moins des mêmes mesures de sécurité que les postes fixes. Même si cela représente une contrainte supplémentaire, les conditions d'utilisation des terminaux nomades imposent même le renforcement de certaines fonctions de sécurité.

#6 : Sensibiliser l'équipe au risque de piratage

Périodiquement, rappelez à votre équipe quelques règles élémentaires : ne pas divulguer des mots de passe à un tiers, ne pas contourner les dispositifs de sécurité internes, éviter d'ouvrir la pièce jointe d'un message venant d'une adresse inconnue, etc. La sensibilisation doit également porter sur **l'utilisation des réseaux sociaux**. « Les comptes Facebook ou LinkedIn des collaborateurs sont des mines d'informations pour les pirates, explique Stéphane Dahan. Ils s'en servent pour adresser des messages très personnalisés qui vont leur permettre d'entrer dans le système d'information de l'entreprise. »...[lire la suite]

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?



Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Cette étude analyse les risques de cyberattaques sur des infrastructures énergétiques européennes, ainsi que leurs potentielles conséquences, notamment sur les réseaux électriques. Elle offre également une approche comparative des mesures prises par différents pays d'Europe afin de protéger leur industrie et collaborer à l'échelle de l'Union européenne.

La digitalisation de l'industrie énergétique permet de révolutionner les processus de production, de stockage, de transport et de consommation d'énergie. Nos infrastructures énergétiques, conçues il y a plusieurs décennies et prévues pour demeurer fonctionnelles pour de nombreuses années encore, côtoient désormais des équipements numériques avec lesquels elles interagissent au quotidien. Ces évolutions, qui sont aujourd'hui un gage de disponibilité, d'efficacité et de réactivité sur toute la chaîne de valeur énergétique, ouvrent pourtant la voie à un type de menace qui jusqu'en 2010 avait relativement épargné cette industrie : les cyberattaques.

Le nombre et la technicité des attaques ont augmenté après les dégâts causés par le virus Stuxnet au sein du complexe d'enrichissement nucléaire iranien de Natanz, bien que cette attaque demeure la plus sophistiquée observée à ce jour. Et s'il y a une réelle prise de conscience des enjeux dans le secteur énergétique, les risques persistent. Les politiques de transition énergétique et les efforts d'intégration des énergies renouvelables ne feront que renforcer cette tendance tant que la cybersécurité ne fait pas partie de la réflexion sur l'avenir du système énergétique.

La réglementation tente de s'adapter, notamment en France où les autorités collaborent étroitement avec les entreprises de l'énergie pour faire émerger un cadre réglementaire contraignant, et protéger les Opérateurs d'Importance Vitale (OIV). Cette démarche inspire également d'autres pays d'Europe, mais des mesures communes à toute l'Union européenne sont à prendre rapidement afin de garantir la sécurité de nos réseaux énergétiques, fortement interconnectés.

LIRE L'ETUDE (PDF)

Original de l'article mis en page : Cyberattaques et systèmes énergétiques: faire face au risque | IFRI – Institut français des relations internationales

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

**Le FBI pourra t-il accéder
aux mails de Gmail ?**



Le FBI
pourra
t-il
accéder
aux
mails de
Gmail ?

Le juge fédéral Thomas Rueter de la cour de Philadelphie a donné son verdict et a statué concernant la saisie de mails depuis des serveurs étrangers, par les autorités américaines. Ce dernier a affirmé : «Même si la récupération de données électroniques par Google à partir de ses multiples centres de données à l'étranger peut en soi représenter un risque d'atteinte à la vie privée, la véritable atteinte intervient au moment de la divulgation aux Etats-Unis».

En gros, le juge fédéral a estimé que le fait d'ordonner à Google de remettre aux autorités les courriers électroniques de sa messagerie Gmail, stockés à l'étranger, n'était pas contraire à la loi. La firme de Mountain View devra se conformer aux mandats et perquisitions du FBI. Google a évidemment déclaré qu'il faisait appel de la décision, en se référant à la jurisprudence Microsoft, car une affaire similaire avait donné raison à Microsoft il y a quelques semaines à New York.

Google devra fournir au FBI les mails hébergés à l'étranger

Google ne souhaite pas livrer au FBI les e-mails stockés hors des Etats-Unis, afin de garantir la vie privée de ses usagers aux quatre coins du monde. Sont concernés par la décision du juge fédéral Thomas Rueter, les six serveurs de l'entreprise présents en Belgique, en Finlande, en Irlande, à Taiwan, Singapour et aux Pays-Bas.

Le juge a estimé qu'« aucune ingérence significative » avec les droits de propriété du titulaire du compte ne pouvait être invoquée concernant les données ciblées, car comme l'a fait remarquer le juge, Google procède déjà régulièrement au transfert de ces données vers ses serveurs aux Etats-Unis, pour ses propres business et sans que les clients en soient forcément informés. Thomas Rueter de la cour de Philadelphie a souligné : « Ces transferts n'interfèrent pas avec l'accès du client ou les droits de propriété des données utilisateur. Même si le transfert interfère avec le contrôle du propriétaire du compte sur ses informations, cette interférence est minime et temporaire ».

Il semble donc que le juge ait retourné les méthodes de Google contre lui-même pour justifier la légalité des saisies des e-mails stockés hors des Etats-Unis au FBI. Du côté de l'entreprise, on s'est contenté de déclarer : « Nous continuerons à repousser les mandats excessifs ».

Original de l'article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l'étranger

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPEEN 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 dessins

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

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

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

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



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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DITP n°93 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

Original de l'article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l'étranger

La liste des zones interdites à la photographie aérienne est publique



La liste des zones interdites à la photographie aérienne est publique

Non, il n'est pas interdit de voler en France ni de prendre des photos aériennes. En revanche, la réglementation encadre strictement l'usage d'un drone et un nouvel arrêté publié le 27 janvier 2017 fixe la liste des zones interdites à la prise de vue aérienne....[Lire la suite]

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

Par des actions 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 sur cette page.



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

RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle pour 2018



RGPD
Règlement
Européen
sur la
Protection
des
Données :
Voici
comment
être en
régle pour
2018

Le GDPR, règlement européen qui renforce le droit des utilisateurs en matière de données personnelles, entrera en vigueur en mai de l'an prochain. D'ici là, 4 actions doivent être menées.

2017 s'annonce chargé pour toutes les entreprises qui collectent et manipulent, de près ou de loin, de la data en provenance de leurs consommateurs. Pour cause, le nouveau règlement européen sur la protection des données personnelles (GDPR) entrera en application le 25 mai 2018. Son objectif est de renforcer les droits des personnes en la matière... et les obligations des entreprises. Voici comment éviter une amende qui sera salée pour les mauvais élèves : 2 à 4% du chiffre d'affaires ou 20 millions d'euros, le montant le plus élevé étant choisi.

Protéger les données personnelles en amont

Commençons par la bonne nouvelle. L'entreprise qui procède à un traitement de données personnelles n'aura plus à remplir de déclaration auprès de la Cnil pour l'en informer, comme elle y est pour l'instant tenue. Ce pilier de la loi « Informatique et liberté » saute.

« Les entreprises doivent 'en échange' se conformer au concept de « privacy by design » érigé par l'article 25 du règlement », explique Matthieu Berguig, avocat spécialisé en droit des nouvelles technologies. Ce concept leur impose de réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service. « Un fabricant d'objets connectés doit donc se poser des questions de base avant de mettre son produit sur le marché : où son stocké les données, par quel protocole de cryptage seront-elles protégées, sont-elles anonymisées... », illustre Matthieu Berguig. Délestée de ce travail de vérification, la Cnil s'évite beaucoup de paperasse... et gagne du temps pour auditer le marché. « On peut être sûrs que les contrôles seront plus nombreux », prévoit Matthieu Berguig.

Nommer un délégué à la protection des données

La Cnil pourra travailler dans cette perspective main dans la main avec un collaborateur d'un nouveau genre, le délégué à la protection des données (DPD). L'article 37 impose sa nomination dans plusieurs cas de figure : lorsque « le traitement est effectué par une autorité publique ou un organisme public », lorsque le traitement impose « un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque le traitement à grande échelle concerne « les catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ». Beaucoup d'entreprises sont donc concernées par l'obligation et toutes sont encouragées à en nommer un.

Chargé de faire respecter le règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, le DPD tient un peu du mouton à cinq pattes. Chez les entreprises déjà bien structurées, le « compliance officer », le collaborateur qui s'assure de la conformité de toute décision business à la législation, sera un candidat naturel à ce rôle de DPD. « Pour toutes les autres, il faut trouver la perle rare, un profil juridique capable également de comprendre les problématiques métiers », note Alan Walter, avocat associé chez Walter Billet Avocats.

Tenir un registre de traitement des données

« En 2017, beaucoup d'entreprises vont s'embarquer dans une totale remise à plat de leurs systèmes de traitement des données à caractère personnel », note Alan Walter. Pour cause, l'article 30 impose aux entreprises de plus de 250 salariés de tenir un registre des traitements effectués. Un registre qui comporte, entre autres, le nom et les coordonnées du responsable du traitement, les finalités du traitement, la catégorie de destinataires auxquels les données à caractère personnel ont été ou seront communiqués. « C'est ce registre qui sera consulté par la Cnil lorsqu'elle voudra entrer en action », précise Matthieu Berguig.

L'article 33 impose d'ailleurs à une entreprise qui a subi une violation de données à caractère personnel d'en notifier l'autorité de contrôle. « Seuls les opérateurs télécoms y étaient jusque-là tenus », note Matthieu Berguig.

Créer une base interopérable pour le droit à la portabilité

L'article 20 du règlement aboutit à la création d'un droit à la portabilité des données personnelles. Si un de vos clients vous quitte pour la concurrence, il a le droit de réclamer le transfert de l'intégralité des données le concernant. « Lorsque cela est techniquement possible », précise l'article. « En d'autres termes, lorsque vous passerez d'une boîte mail à une autre, vous aurez théoriquement le droit d'importer tout votre historique de mails », illustre Matthieu Berguig. Une obligation dont la mise en place pourrait être techniquement compliquée dans de nombreux cas.

Alan Walter souligne un autre écueil, juridique celui-ci, en prenant l'exemple de l'un de ses clients, courtier en assurance pour expatriés. « Les données qu'il recueille sont très sensibles car elles concernent le domaine médical. Elles ne peuvent être transmises à n'importe qui, du fait du secret médical. Donc comment doit-il faire ? », s'interroge-t-il. Dans ce cas, il faudrait s'assurer que le destinataire des données offre les garanties nécessaires pour qu'il ne soit pas porté atteinte aux droits des personnes concernées. Problématique d'autant plus épineuse avec des transferts de données qui sont susceptibles d'intervenir vers des opérateurs situés hors de l'Union européenne et donc soumis à des droits différents. Premiers éléments de réponse début mai 2018.

Original de l'article mis en page : Protection des données : voici comment être en règle pour 2018

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

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

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETEP n°33 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

Comment devenir DPO Délégué à la Protection des Données dans le cadre du RGPD, Règlement européen de protection des données ?

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	 SPY DETECTION Services de detection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI VOUS INFORME		Comment devenir DPO Délégué à la Protection des Données dans le cadre du RGPD, Règlement européen de protection des données ?			

Entré en vigueur en mai dernier, le Règlement général sur la protection des données impose de nouvelles règles en matière de gestion des données personnelles. Avec l'obligation pour les entreprises de se mettre en conformité avant mai 2018. Ce qui implique une modification des contrats fournisseurs.

Qui est concerné?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »
Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne.
Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

Qu'est-ce qu'une donnée à caractère personnel?

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement.
Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel.
Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées.

Quelles obligations pour les entreprises?

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation...), mais aussi les contrats passés avec les fournisseurs et clients sont impactés (voir encadré ci-dessous).
« Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).
Le RGPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilités en fonction de la mainmise de chacun sur les données. Cette notion de coresponsabilité doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs: en effet, le sous-traitant désigné par une organisation pour assurer le traitement des données devient, avec le RGPD, coresponsable de la légalité des traitements. Il sera donc tenu d'informer ses clients et de tenir des registres pour recenser les données, ainsi que d'accepter les audits demandés par son client pour s'assurer de la conformité des traitements.
Les sous-traitants concernés peuvent être, par exemple, l'éditeur d'un CRM en ligne, le routeur d'une campagne d'e-mailing, un service de relation client, etc. Le responsable du traitement, de son côté, doit s'assurer que ses fournisseurs ont pris les mesures nécessaires pour assurer la sécurité des données.
Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement. Quel impact sur les contrats fournisseurs? Pour se mettre en conformité avec le RGPD, les directeurs achats devront veiller à renforcer les contrats passés avec leur fournisseurs...

Le délégué à la protection des données

- Le règlement européen consacre la fonction de Délégué à la Protection des Données (DPO ou en anglais DPO) dans les organismes.
Les responsables de traitement et les sous-traitants devront obligatoirement désigner un DPO :
1. s'ils appartiennent au secteur public,
 2. si leur activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
 3. si leur activité principale les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

Les responsables de traitement peuvent opter pour un DPO mutualisé ou externe.

- Véritable « chef d'orchestre » de la conformité en matière de protection des données, le DPO est chargé :
1. d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
 2. de contrôler le respect du règlement et du droit national en matière de protection des données ;
 3. de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA ou EIVP) et d'en vérifier l'exécution ;
 4. de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

QUI PEUT ÊTRE DPO ?

Le DPO est désigné sur la base de son expertise.

CONSEILS POUR LA MISE EN PLACE DU FUTUR DPO

- Compte tenu que jusqu'au 25 mai 2018, le non respect de la Loi Informatique et Libertés est passible de 5 ans de Prison et jusqu'à 300 000 euros d'amende, nous vous conseillons fortement d'entamer au plus vite les démarches suivantes déclarer un CIL avant le 25 mai 2018 ou désigner un DPO après. Puis :
1. Réaliser ou faire réaliser un indispensable état des lieux (appelé aussi audit) afin d'identifier l'ensemble des traitements de données personnelles et l'ensemble des lieux dans lesquels des données personnelles sont traitées ;
 2. Identifier dans la Loi Informatique et Libertés ou dans le RGPD des particularités propres à votre métier qui vous autorise à certains traitements interdits à d'autres activités ou qui nécessiteraient une demande d'autorisation ;
 3. Faire une analyse de risque autour des traitements et des données personnelles présentes dans votre établissement. Cette étape indispensable peut être assurée par notre Expert Denis JACOPINI, Certifié ISO 27005 Risk Manager ;
 4. Porter au registre l'ensemble des traitements identifiés ;
 5. Mettre en conformité les traitements qui ne respectent pas la loi ou le règlement.
 6. Suivre régulièrement l'évolution des traitements au sein de l'organisme.

Articles du règlement associés

Article 13 | Article 14 | Article 30 | Article 33 | Article 35 | Article 36 | Article 37 | Article 38 | Article 39 | Article 47 | Article 57

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.



DESIGNATION
N° DPO-15945



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)

Twitter s'appuie sur l'intelligence artificielle pour lutter contre le harcèlement



Le réseau social va s'aider d'outils d'apprentissage automatique pour repérer plus vite les messages allant à l'encontre de ses règles d'utilisation. Un concert d'excuses et quelques mesures concrètes....[Lire la suite]

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

Par des actions 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 sur cette page.



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

Un collectif Anonymous pirate

le site de l'Anssi



Un
collectif
Anonymous
pirate le
site de
l'Anssi

Cible d'une attaque DDoS, le site Internet de l'Agence nationale de la sécurité des systèmes d'information (Anssi) a été bloqué à plusieurs reprises les 4 et 5 février.

Trois semaines après l'annonce d'une campagne de recrutement, l'Agence nationale de la sécurité des systèmes d'information (Anssi) fait les frais de sa popularité grandissante. Cible d'une attaque par déni de service distribué (DDoS), le site Internet de l'Anssi a été bloqué le 4 février au soir, rapporte Zataz, et a été à nouveau perturbé ce vendredi 5 février après-midi jusqu'à 15h30 environ.

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Le site de l'Anssi piraté par un collectif Anonymous

Google sommé de livrer des mails stockés à l'étranger



Google
sommé de
livrer des
mails
stockés à
l'étranger

Contredisant une jurisprudence Microsoft, un juge a ordonné à Google de livrer les mails stockés sur des serveurs en dehors des Etats-Unis. La firme a fait appel.



Décidément la jurisprudence américaine sur l'extraterritorialité des mandats de perquisitions sur les données conservées hors des Etats-Unis joue à la girouette. A la fin janvier, Microsoft gagnait une seconde victoire sur ce sujet. Les juges de la Cour d'Appel de New York ont jugé, dans la douleur, que le Secure Communications Act (SCA) sur lequel se base les mandats n'avait pas en 1986 été conçu pour des données localisées hors du territoire américain.

Une jurisprudence mise à mal par une autre affaire concernant Google. Ce dernier a été sollicité par le FBI dans une affaire de fraude datant du 2 août 2016 et une autre du 19 août portant sur un vol de données industrielles sur le territoire américain. Mais certaines données des comptes des suspects étaient disséminées sur des datacenters de Google à l'étranger. La firme américaine a expliqué que pour des raisons de performances, les courriers électroniques pouvaient être découpés en petits morceaux et stockés sur différents serveurs à l'étranger. La firme de Mountain View s'appuyait donc sur les décisions favorables à Microsoft en matière de non extra-territorialité des mandats de perquisition pour refuser le mandat du FBI.

Une violation de la vie privée aux États-Unis

Mais le juge, Thomas Rueter, du tribunal de Philadelphie, en a décidé autrement. Il considère en effet que « le fait de transférer électroniquement des données d'un serveur dans un pays étranger vers le datacenter de Google en Californie ne constitue pas une saisie ». Cette notion de saisie est définie par le 4^{ème} amendement de la Constitution américaine qui stipule, « le droit des citoyens d'être garanti dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir ». La qualification de saisie n'est pas retenue par le juge, car « il n'y a aucune interférence significative avec l'intérêt possessif du titulaire du compte dans les données utilisateur ». Il poursuit en expliquant que Google transfère régulièrement des données entre ses installations sans que les utilisateurs en soient mis au courant et cela ne les empêche pas d'accéder à leur données, ni ne remet en question leur droit de propriété. Et si interférence il y a, elle est « minime et temporaire ». Pour motiver sa décision, le juge Rueter, précise que « même si la récupération des données électroniques par Google depuis ses multiples centres de données à l'étranger a le potentiel d'une invasion de la vie privée, la violation réelle de la vie privée se produit au moment de la divulgation aux États-Unis ». Pour lui, la perquisition et la saisie ont eu lieu aux Etats-Unis et non à l'étranger, le mandat de perquisition est alors contraignant pour Google. Ce dernier a déjà annoncé sa décision de faire appel de ce jugement.

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Google sommé de livrer des mails stockés à l'étranger

Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien



Souhaitant mettre rapidement sur le marché leurs produits, les fabricants d'objets connectés ont eu tendance à négliger l'aspect sécurité, contribuant ainsi à la vulnérabilité de leurs utilisateurs face à de possibles attaques.

Atlantico : En septembre et octobre 2016, deux attaques DDOS ont été particulièrement marquantes : la première sur l'entreprise OVH et la deuxième sur DYN. Dans les deux cas, ces attaques ont été rendues possibles par les objets connectés. Malgré l'ampleur de ces attaques, celles-ci sont à relativiser. Dans une récente étude réalisée pour le compte de l'entreprise HSB, on note que seulement 10% des utilisateurs ont été touchés par des problèmes de piratage. Quels sont les risques du piratage des objets connectés ?

Quel peut être le préjudice porté aux particuliers et aux entreprises ?

Yvon Moysan : Une attaque DDoS ou attaque par déni de service massive vise à rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement. Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément et depuis de multiples endroits. L'intensité de ce « tir croisé » rend le service instable, voire indisponible. **Le risque d'être confronté à ce type d'attaque est important et surtout les tentatives sont nombreuses.** Dans le cas de la société américaine Dyn que vous évoquez, celle-ci a été victime d'une attaque de plus d'un Téra-octet par seconde, ce qui pourrait concerner environ 10 millions d'objets connectés piratés. Ce niveau d'intensité est toutefois très rare.

Le préjudice subi dépend du type d'objets connectés piratés et du caractère sensible des données des particuliers. Si la majorité des objets connectés contiennent rarement des informations aussi sensibles que celles qui sont stockées sur un ordinateur, il en existe des sensibles comme les voitures connectées ou les fusils intelligents qui, piratés à distance, peuvent représenter un véritable danger, potentiellement mortel pour l'utilisateur. Et ce risque s'est d'ores et déjà avéré. Des experts en sécurité informatique ont ainsi réussi à prendre le contrôle à distance d'une Jeep Cherokee. Ils ont pu agir sur la vitesse, freinant et accélérant à leur guise, envoyant même la voiture dans le fossé alors que pour le fusil intelligent, d'autres experts ont réussi à bloqué le déclenchement du tir.

Le risque existe également pour des objets plus communs comme les applications de smart home. Des hackers ont ainsi réussi à bloquer la température de thermostats connectés à une température polaire ou saharienne. Plus préjudiciable, des hackers ont pris le contrôle de caméras de surveillance, récupéré les vidéos enregistrées, et au final les ont diffusées sur le Web. Un baby phone a également été la cible d'un hacker terrorisant un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, celui-ci s'est mis à hurler des insanités sur le nourrisson. **Le risque peut surtout être généralisé si des hackers réussissent à prendre le contrôle des réseaux d'électricité ou de gaz sur un quartier par exemple.** Il devient en effet possible de plonger toute une zone dans le noir ou, en fonction des données récoltées sur la consommation, de savoir quelles habitations sont occupées ou pas, en vue d'éventuels cambriolages.

Cela peut ensuite être contraignant pour la société qui a fabriqué et vendu les objets piratés car cela révèle la faiblesse du niveau de sécurité. Dans le cas de l'attaque de la société Dyn, une partie des objets connectés étaient ceux de la société chinoise Xiongmai, qui a dû les rappeler en urgence pour leur appliquer un correctif de sécurité. Cela peut aussi être problématique pour les clients de la société victimes de l'attaque. Dans le cas de Dyn, cela a eu pour conséquence de rendre inaccessible pendant une dizaine d'heures des sites comme Twitter, Ebay, Netflix, GitHub ou encore PayPal.

On peut aussi s'interroger sur certaines pratiques des constructeurs. Le fait de mettre un mot de passe commun à tous les appareils avant une première connexion a déjà été pointé du doigt. Quels autres dysfonctionnements peut-on mettre en avant ? Face à l'augmentation du nombre d'objets connectés, comment s'adaptent précisément les constructeurs en termes de sécurité ?

Tout d'abord il est important de préciser que ce type d'attaques par déni de service n'a rien de nouveau : les cybercriminels utilisent depuis des années des armées d'ordinateurs piratés pour inonder de requêtes les sites ciblés et les rendre inaccessibles.

La nouveauté réside ici dans le nombre croissant des objets connectés qui accroît de manière exponentielle les possibilités d'attaques. Or la puissance d'une attaque dépend essentiellement du nombre de périphériques piratés, d'où l'intérêt de passer par les objets connectés. Il existe en effet plusieurs milliards d'objets connectés dans le monde contre quelques centaines de millions d'ordinateurs. Pour y faire face, il existe des solutions proposées par les hébergeurs pour protéger leurs serveurs des attaques. Ces solutions permettent, par exemple, d'analyser en temps réel et à haute vitesse tous les paquets, et si besoin d'aspirer le trafic entrant, voire de mitiger, c'est-à-dire repérer tous les paquets IP non légitimes, tout en laissant passer les paquets IP légitimes.

Du côté des constructeurs d'objets connectés, tous les thermostats, toutes les webcams ou les imprimantes ne présentent pas de faille de sécurité, mais il s'agit d'un point préoccupant car pour la plupart des fabricants, la sécurité n'a pas été la priorité dès le départ, ayant souvent été donnée à la rapidité de la mise à disposition du produit sur le marché pour répondre à un nouveau besoin. Il faudrait que des normes minimales de sécurité puissent être définies comme le cryptage des données échangées sur le réseau ou l'exigence de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance et l'interdiction de mots de passe comme « 123456 » particulièrement vulnérables. Dans cet esprit, la Online Trust Alliance, qui regroupe des éditeurs comme Microsoft, Symantec (Norton) et AVG, a rédigé un guide des bonnes pratiques pour minimiser les risques de piratage. Les constructeurs d'objets connectés peuvent, par ailleurs, faire évaluer leurs systèmes de cryptage par des sociétés spécialisées, pour identifier les éventuelles vulnérabilités.

Comment se prémunir du piratage d'objets connectés ? Quels sont les bons comportements à adopter ? Que faire en cas de doute ?

Du côté des particuliers, il apparaît préférable de privilégier les produits de sociétés à la pointe des questions de sécurité informatique, comme Google ou Apple. Il faut également installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle. Pour finir, il faut limiter l'accès d'un objet connecté aux autres objets connectés dans la maison. Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau. Par exemple, il n'est pas vraiment nécessaire que l'imprimante soit connectée à la télévision.

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

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

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Le Net Expert

INFORMATIQUE

Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Attention danger :
apprenez à vous protéger contre le piratage de vos objets
connectés du quotidien | Atlantico.fr