

RGPD : les changements à prévoir pour se conformer à la protection des données personnelles



A partir du 25 mai 2018, toutes les entreprises gérant et collectant des données sur les personnes devront respecter chacune des obligations du Règlement européen pour la protection des données, le RGPD. Toutes les entreprises sont donc concernées par ce règlement que vous fassiez de l'outbound ou de l'inbound marketing. Le règlement prévoit également de lourdes sanctions en cas de violation de clauses : votre entreprise est-elle prête ?

1-QU'EST-CE QUE LE RGPD ?

Le Règlement général pour la protection des données – RGPD – a été adopté par le Parlement européen le 4 avril 2016. En anglais Il est le GDPR pour « General Data Privacy Regulation ». Il vise à protéger toutes les données à caractère personnel des individus au sein de l'Union Européenne à travers trois objectifs ambitieux et précis :

- L'uniformisation européenne de la réglementation sur la protection des données
- La responsabilisation des entreprises
- Le renforcement du droit des personnes



Le règlement n'a besoin d'aucune transposition légale en fonction du pays de l'entreprise : son application concerne directement tous les pays européens, à partir d'un même texte. L'intérêt majeur de cette uniformisation à échelle européenne est la simplification des mesures, centralisées vers un interlocuteur unique. Les entreprises pourront s'adresser directement à l'autorité de protection des données pour l'Etat membre dans lequel se situe l'établissement principal. La simplification des formalités pour les entreprises doit aussi permettre de les responsabiliser dans le traitement et la gestion des données. Les rôles, les responsabilités, les fonctions sont réparties et précisées, avec un ensemble de points à suivre : chaque entreprise doit mettre en place une politique de protection des données personnelles, et s'assurer qu'à chaque étape de la gestion des données, le RGPD est respecté.

De nouveaux droits sont introduits, comme le droit à la portabilité, qui permet aux personnes de récupérer les données fournies, pour un contrôle total de ses propres données. On peut citer aussi le droit à réparation des dommages matériels et moraux, des droits spécifiques pour les enfants et le traitement de leurs données, des droits aux recours collectifs.



2 – LE RGPD, POUR QUOI ?

Le RGPD est applicable sur toutes les données à caractère personnel de chacun des citoyens et résidents européens, soit « toute information se rapportant à une personne physique identifiée ou identifiable » selon la définition du RGPD. Il permet même de faire valoir ses droits face à une entreprise non européenne.

Dès lors qu'une entreprise européenne traite des données personnelles – noms, e-mails, numéro de téléphone... elle est concernée. Collecte, enregistrement, conservation, classement, utilisation, diffusion... le RGPD s'applique aux entreprises privées comme publiques des 28 Etats-membres de l'Union européenne, ou pour être plus précis :

- Aux entreprises proposant des biens et des services sur le marché européen
- Aux entreprises collectant des données à caractère personnel sur les résidents de l'UE
- Aux entreprises non implantées dans l'UE, dès qu'elles collectent et traitent de données personnelles appartenant à un résident de l'Union européenne...[lire la suite]

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

Besoin d'une formation pour apprendre à vous

mettre en conformité avec le RGPD ? ?

Contactez-nous

A lire aussi :

Mise en conformité RGPD : Mode d'emploi

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

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

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

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

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



Réagissez à cet article

Source : RGPD : les changements à prévoir, comment se conformer sur la protection des données personnelles ?

La protection des données personnelles a 40 ans. Retour sur ses origines en vidéo



A l'occasion de ses 40 ans, la CNIL vous propose une sélection d'archives vidéos concoctée par l'INA ! Ces temps-forts télévisuels retracent l'action de la CNIL et les grands sujets qui ont marqué son histoire.

Consultez la liste de nos formations et services sur le RGPD



RGPD = RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

LE NET EXPERT

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

Besoin d'un Expert ? contactez-nous

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

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



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



Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en
Protection des Données Personnelles

Contactez-nous



Réagissez à cet article

Source : ARCHIVES | La CNIL, 40 ans au service des libertés !
| CNIL

RGPD : Faire face aux exigences

Denis JACOPINI



vous informe

RGPD : Faire aux
face exigences

Faire aux

RGPD : Faire aux
face exigences

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

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

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

Tous les flux de données sont concernés par cette nouvelle réglementation.

Ces nouvelles contraintes s'appuient notamment sur le principe d'accountability qui impose à chaque entreprise une obligation de rendre compte, notamment en se dotant d'une politique globale de protection des données conforme à la réglementation, et en étant à même de prouver à tout moment que des mesures concrètes et des procédures adéquates ont été mises en place. Dans ce nouveau contexte, il est préconisé que les responsables de traitement aient recours à des prestataires externes leur permettant d'assurer une mise en conformité effective...[lire la suite]

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



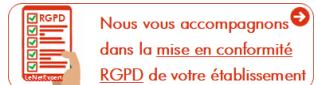
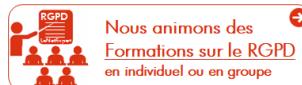
DÉSIGNATION
N° DPO-15945



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)

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

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

A screenshot of a television news program. The top left corner displays the name "Denis JACOPINI". Below it, the channel logo "8 LE JT" is shown. A small portrait of Denis Jacopini is visible. The bottom left of the screen contains the text "DENIS JACOPINI PAR TÉLÉPHONE EXPERT INFORMATION ASSOCIATION AUPRÈS DES TERRITOIRES" and "TÉLÉPHONE PROTÉGÉ ET GRATUIT". The bottom right corner shows the time "20:52". The bottom of the screen features the text "vous informe" in blue.

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

Article original : La gazette des communes

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

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

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

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

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

Besoin d'une formation pour apprendre à vous

mettre en conformité avec le RGPD ?

Contactez-nous

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

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

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

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

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

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



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

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

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

25% des cyberattaques cibleront les objets connectés en 2020

A screenshot from a LCI news program. On the left, there's a video frame showing Denis JACOPINI, a man with dark hair and a beard, wearing a dark suit and tie, sitting at a desk. Above the video, his name "Denis JACOPINI" is written in blue. Below the video, the text "VOUS INFORME" is displayed in white. In the bottom left corner of the video frame, the LCI logo is visible. On the right side of the image, there is a large, bold, orange text overlay that reads "25% des cyberattaques cibleront les objets connectés en 2020".

Denis JACOPINI

VOUS INFORME

LCI

25% des cyberattaques cibleront les objets connectés en 2020

L'IoT présente des problématiques de sécurité particulièrement épineuses. La majorité des objets connectés ont fait l'impasse sur la sécurité, avec des options de configuration minimales, voire inexistantes sur le sujet, et une absence de protocoles d'authentification ou d'autorisation. La majorité des objets connectés ne dispose pas d'interface qui permet aux outils de sécurité de s'y installer, ce qui rend quasi-impossible le patching et les mises à jour. Dans ce contexte, il n'est guère étonnant que les experts s'attendent à ce que 25% des cyberattaques ciblent l'Internet des Objets en 2020.

L'expansion des réseaux IoT (objets connectés) instaure de nouvelles menaces pour la sécurité avec environ 22,5 milliards d'appareils connectés prévus d'ici 2021, selon un rapport de Business Insider. La sécurité représentera donc un défi de taille, mais les gros volumes de données engendrés par l'IoT pourraient en réalité aider les chercheurs à repérer les failles de sécurité. Encore faudrait-il que les entreprises déclenchent enfin une cartographie rigoureuse de leur patrimoine informationnel. Selon une nouvelle étude de CyberArk, près de deux tiers des organisations françaises (62 %) ayant été victime d'une cyberattaque n'ont pas avoué à leurs clients que leurs données personnelles avaient été compromises. Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en mai 2018, les entreprises qui n'agiront pas pour être plus transparentes s'exposeront à d'importantes sanctions. La mise en place du RGPD / GDPR en mai 2018 les incite fortement »...[lire la suite]

LE NET EXPERT

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

Besoin d'un Expert ? contactez-nous

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

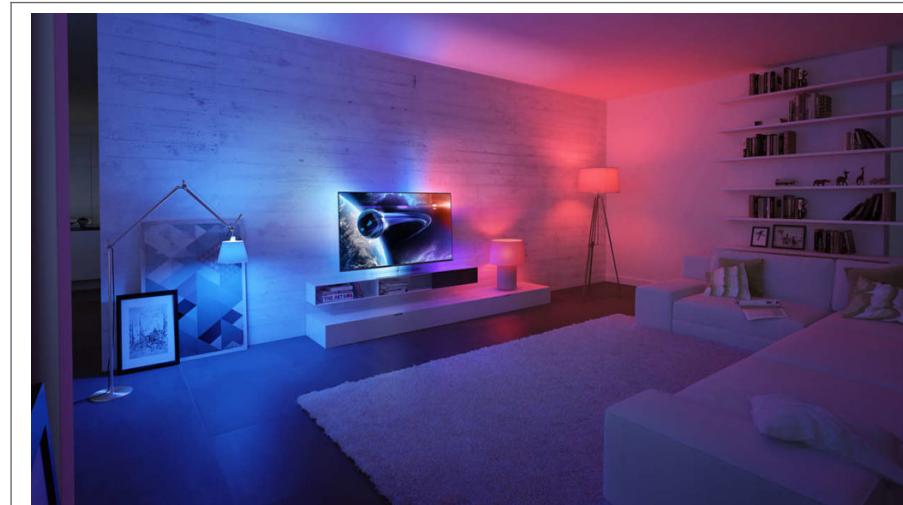
Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



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

Source : Cyberisques News – Cybersécurité : 25 Prévisions utiles pour 2018

Cadeaux de noël : Comprendre les risques liés aux objets connectés, c'est déjà commencer à se protéger



Cadeaux de
noel
Comprendre les
risques liés
aux objets
connectés
c'est déjà
commencer à se
protéger

Les années passent et les scandales de sécurité et de vie privée se succèdent à un rythme qui ne semble pas réduire. L'un des secteurs des technologies de l'information semble concentrer la plupart des problèmes : les objets connectés

Récemment, la CNIL a pointé du doigt des jouets connectés a priori inoffensifs. Le problème ? Ces poupées, équipées de caméra, d'un micro et d'un haut-parleur constituent un cheval de Troie idéal pour n'importe quelle personne malveillante. Ok, mais ont-elles été l'objet d'un piratage ? Pas encore mais un produit similaire s'est récemment fait pirater causant la publication d'un peu plus de 2 millions de messages intimes sur Internet.

Avant de céder à la panique et de déménager dans un joli mais vieux corps de ferme dans le Vercors, quelques ajustements semblent nécessaires...[lire la suite]

LE NET EXPERT

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

Besoin d'un Expert ? contactez-nous

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

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



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

Source : Comprendre les risques liés aux objets connectés, c'est déjà commencer à se protéger – Tech – Numerama

Le RGPD (GDPR en anglais) : une réglementation que doivent aussi suivre vos sous-traitants

A video still from a French news program. On the left, there is a portrait of Denis JACOPINI, a man with dark hair and a beard, wearing a dark suit and tie. He is looking slightly to his left. To his right, the text "Denis JACOPINI" is written in blue. Below the portrait, the words "VOUS INFORME" are displayed in white on a dark background. In the bottom left corner of the video frame, the letters "LCI" are visible.

Le RGPD (GDPR en
anglais) : une
réglementation que
doivent aussi suivre vos sous-
traitants

Le nouveau règlement européen sur la protection des données personnelles doit entrer en vigueur en mai 2018. Les donneurs d'ordre des métiers de service ont préparé leur mise en conformité et pressent leurs sous-traitants de faire de même. Cela représente pour eux de nouvelles charges à assumer.

Denis JACOPINI nous rappelle un extrait des termes de l'article 28 du RGPD (Règlement Européen sur la Protection des Données) :

Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Le traitement par un sous-traitant est régi par un contrat [...] prévoit, notamment, que le sous-traitant:

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;

c) prend toutes les mesures requises en vertu de l'article 32;

d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant;

e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;

f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant;

g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel; et

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

Ainsi, même si vous êtes en règle vis à vis du RGPS mais si votre sous-traitant ne l'est pas, le résultat pourrait bien être équivalent comme si vous n'étiez pas en règle.

La mise en conformité du sous-traitant requiert d'abord une mise à niveau des mesures organisationnelles et techniques de cyber sécurité, avant de se concentrer sur la gestion des données personnelles. Les PME et ETI ont souvent fait l'impasse sur ce domaine générateur de coûts, pensant, grâce à leur petite taille, d'échapper aux attaques les plus graves. Aujourd'hui avec les puissants moyens d'information, ce n'est plus le cas, un pirate peut appréhender une filière et frapper le maillon le plus faible...[lire la suite]

LE NET EXPERT

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

Besoin d'un Expert ? contactez-nous

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

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



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

Source : *Le GDPR, un risque pour les PME en position de sous-traitance ?*

Formation RGPD : Ce n'est pas qu'une affaire de juristes



**Formation RGPD
: Ce n'est pas
qu'une affaire
de juristes**

Le 25 mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Les 6 étapes recommandées par la CNIL pour vous préparer au RGPD sont :

1- DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

2- CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

3- PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

4- GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

5- ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire).

6- DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Pour cartographier vos traitements de données personnelles, vous devrez avoir une méthode, des outils, collecter des informations à la fois techniques et organisationnelles.

Pour prioriser les actions à mener vous devrez identifier précisément les traitements à risques, les données sensibles et connaître les solutions techniques applicables.

Pour gérer les risques, vous devrez appliquer une méthode relative à cette obligation. Proche de la méthode EBios, l'analyse d'impact relative à la protection des données (DPIA) est le passage obligatoire pour tout organisme (entreprise ou association) disposant de salariés ou détenant des données sensibles appartenant à des tiers.

L'organisation des processus internes nécessite une excellente connaissance des menaces et des risques. Une certification relative à une norme ISO 27001 ou 27005 nous paraît essentielle.

Vous pouvez donc constater que pour chacun des points ci-dessus, le chef d'orchestre que doit être le DPO doit à la fois avoir une bonne connaissance du règlement Européen RGPD (ou GDPR en anglais) mais également connaître et maîtriser différents sujets tels que la sécurité informatique, différentes méthodes telles que l'analyse des flux de données et l'analyse de risques.

Ainsi, nous considérons qu'il serait inconscient d'aborder la mise en conformité avec le RGPD des établissements sans action conjointe d'un conseil juridique spécialisé en droit des données personnelles et d'une personne ayant une bonne connaissance de la sécurité informatique et de l'analyse de risques autour de des données.

Ceci n'est que mon avis, n'hésitez pas à me faire part du votre ou commenter ce post.

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

CONTENU DE NOTRE FORMATION RGPD :

Parce que les piratages sont de plus en plus fréquents et dangereux, à tout moment, nos données personnelles médicales, bancaires et confidentielles peuvent se retrouver dans la nature à cause d'un professionnel négligent ayant manqué à son obligation de sécurité des données vis-à-vis de ses clients, salariés, fournisseurs...

Pour ne pas que vous deveniez ce professionnel négligent risquant d'être sanctionné pénallement et par une mauvaise réputation, un règlement Européen (le RGPD) entrant en application le 25 mai 2018, clarifie les obligations que tous les professionnels devraient déjà respecter.

Venez découvrir lors de cette journée de formation les points importants de ce règlement Européen et la méthode à suivre pour continuer sereinement votre activité.

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

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

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

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

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

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



Denis JACOPINI est Expert Judiciaire en Informatique

spécialisé en « Sécurité » « Cybercriminalité » et en

protection des « Données à Caractère Personnel ».

▪ Audit Sécurité (ISO 27005) ;

▪ Expertise technique et judiciaire (avis

techniques, recherche de preuves téléphones,

disques durs, e-mails, conteneurs, détournements

de clientèle...) ;

▪ Expertise de systèmes de vote électronique ;

▪ Formations et conférences en cybercriminalité ;

(Autorisation de la DRCR n°93 84 03041 84)

▪ Formation de C.I.L. (Correspondants Informatique

et Libertés) ;

▪ Accompagnement à la mise en conformité CNIL de

votre établissement.

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

RGPD : Ca ne se passera plus comme ça !



Selon une nouvelle étude de CyberArk, près de deux tiers des organisations françaises (62 %) ayant été victime d'une cyberattaque n'ont pas avoué à leurs clients que leurs données personnelles avaient été compromises. Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en mai 2018, les entreprises qui n'agiront pas pour être plus transparentes s'exposeront à d'importantes sanctions.

« Malheureusement, il n'est pas rare que les organisations décident de cacher l'ampleur des dégâts causés par une cyberattaque. Comme nous l'avons vu lors des violations de données chez Yahoo !, Uber et bien d'autres, les entreprises peuvent soit dissimuler des informations intentionnellement, soit constater que l'attaque a finalement été plus nuisible que précédemment annoncé, déclare Jean-François Pruvot, Regional Director Europe West and South Europe, Sales chez CyberArk. Dès l'année prochaine, ce type de comportement sera lourdement sanctionné, en raison des amendes qui seront infligées en vertu du RGPD en cas de manque de conformité. L'autre point étonnant de cette étude réside dans cette obstination à appliquer des pratiques dépassées en matière de sécurité, et le manque de cohésion entre les leaders commerciaux et les responsables de la sécurité IT, malgré leur capacité à identifier les risques encourus et les cyberattaques qui font sans cesse la une des journaux. »...[lire la suite]

Complément de Denis JACOPINI :

À partir du 25 mai 2018 les entreprises, filiales ou agences françaises ont obligation de signaler à la CNIL tout vol de données ou piratage ayant entraîné une exposition des données détenues auprès de personnes non autorisées.

Pour qu'il y ait violation, 3 conditions doivent être réunies :

- Vous avez mis en œuvre un traitement de données personnelles ;
- Ces données ont fait l'objet d'une violation (destruction, perte, altération, divulgation ou un accès non autorisé à des données personnelles, de manière accidentelle ou illicite) ;
- Cette violation est intervenue dans le cadre de votre activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de votre service de téléphonie ou d'accès à d'internet).

La notification doit être transmise à la CNIL dans les 24h de la constatation de la violation. Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

Une notification initiale dans les 24 heures de la constatation de la violation ;

Puis, une notification complémentaire dans le délai de 72 heures après la notification initiale.

Le formulaire à utiliser est celui-ci :



https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

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

Besoin d'une formation pour apprendre à vous

mettre en conformité avec le RGPD ?

Contactez-nous

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

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

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

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

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

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



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

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



Source : CNIL et *Enquête CyberArk* : 62 % des entreprises françaises n'ont pas signalé des violations de données à leurs clients – *Global Security Mag Online*

Webmaster ou responsables de sites : comment répondre aux demandes d'effacement de données personnelles publiées sur votre site ?



Webmaster ou responsables de sites : comment répondre aux demandes d'effacement de données personnelles publiées sur votre site ?

Tout internaute a la possibilité de demander à un responsable de site Internet que ses données personnelles ne soient plus diffusées en ligne, et que les pages diffusant ces données ne soient plus indexées par les moteurs de recherche.

En tant que responsable d'un site internet, comment répondre à ces demandes ?

Le règlement européen sur la protection des données qui entre en vigueur en mai 2018 modifie les modalités d'exercice du droit d'opposition qui sera prévu à l'article 21 et introduit un droit à l'effacement à l'article 17.

- Une demande d'opposition ne sera plus soumise à la justification de motifs légitimes.

• En conséquence, dès qu'il sera saisi d'une telle demande, le responsable de traitement ne devra plus traiter les données, sauf à prouver qu'il existe des motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou pour la constatation, l'exercice ou la défense de droits en justice.

• Cette demande devra être traitée « dans les meilleurs délais » et sous 1 mois maximum à compter de la réception de la demande (article 12) contre 2 mois aujourd'hui.

Je reçois un courrier me demandant de supprimer des données personnelles que faire ?

Etape 1 : vérifier que la demande est complète

Une demande d'opposition de la part d'un internaute doit comporter a minima :

- Le motif de la demande (jusqu'au 25 mai 2018, date d'entrée en vigueur du règlement européen)

• Un moyen d'identifier le demandeur (ex. copie d'un justificatif d'identité : une copie noir et blanc du recto suffit, vous ne devez pas conserver cette pièce au-delà du temps nécessaire pour traiter la demande). L'identification du demandeur peut également être réalisée par la mise en place d'une procédure ad hoc par le responsable de traitement.

Etape 2 : répondre par écrit à la demande

Vous disposez d'un délai légal de 1 mois à compter de la date de réception du courrier pour répondre à la demande.

3 options s'offrent à vous :

- Demander des compléments si la demande est imprécise ou incomplète (absence du justificatif d'identité par exemple). Vous devez répondre au demandeur en lui précisant les compléments à vous fournir pour pouvoir traiter sa demande. Vous pouvez également lui demander toute précision utile vous permettant de faciliter le traitement de la demande (urls précises faisant l'objet de la demande, inventaire des données à effacer...). Lorsque vous demandez des compléments, le délai est suspendu et court à nouveau une fois ces éléments fournis par le demandeur.

• Refuser de donner suite à la demande de l'internaute. Dans ce cas, vous devez répondre par écrit au demandeur et impérativement motiver votre décision de refus.

• Répondre positivement à la demande. Dans ce cas, vous procéderez en 3 temps :

1. En supprimant ou modifiant les pages en cause de votre site Internet

2. En procédant à la mise à jour du cache des moteurs de recherches.

3. En confirmant la suppression ou la modification au demandeur

Comment répondre favorablement à une demande d'opposition ?

En fonction de la demande de l'internaute (suppression du contenu, correction, anonymisation, désindexation des moteurs de recherches) vous disposez de différentes solutions pour y répondre.

Tout contenu web a par défaut vocation à être indexé par les moteurs de recherche. Ainsi, la prise en compte effective d'une demande d'opposition à la diffusion en ligne de données personnelles implique, outre la suppression ou modification du contenu, de s'assurer également de sa désindexation par les moteurs de recherche...[lire la suite]

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

Besoin d'une formation pour apprendre à vous

mettre en conformité avec le RGPD ??

Contactez-nous

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

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

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

DIRECTIVE (UE) 2016/680 DU PARLEMENT 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 étapes

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

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

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

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



Denis JACOPPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des données à caractère personnel ».

Autres Services (DSI) :

- Expertises techniques et judiciaires (avis techniques, Recherche de preuves téléphoniques, analyse de logiciels, conteneurs, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de CIL (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : Webmaster ou responsables de sites : comment répondre aux demandes d'effacement de données personnelles publiées sur votre site ? | CNIL