

Utilisation des données personnelles dans le cas de la prospection Téléphonique – Rappel des règles | Denis JACOPINI



Dans le cadre de vos activités, vous pouvez être amenés à contacter par téléphone des personnes.
Quelles sont les règles à respecter ?

LE PRINCIPE : Information préalable et droit d'opposition.

La prospection par téléphone (télémarketing) est possible à condition que la personne soit, au moment de la collecte de son numéro de téléphone :

- informée de son utilisation à des fins de prospection.
- en mesure de s'opposer à cette utilisation de manière simple et gratuite, notamment par le biais d'une case à cocher.

LÉGISLATION APPLICABLE

Article 38 de la loi Informatique et Libertés du 6 janvier 1978

Articles L.34 et R.10 du code des postes et des communications électroniques.

RÉFÉRENCES UTILES

Code Déontologique du e-commerce et de la vente à distance du FEVAD

SANCTIONS

Amende de 750 € par appel

dans le cas de l'utilisation des coordonnées des personnes inscrites sur la « Liste Orange », à partir des annuaires téléphoniques (contravention de la 4e classe prévue par l'article R.10-1 alinéa 1 du code des postes et des communications électroniques).

5 ans emprisonnement et 300 000 € amende

Délit prévu par les articles 226-18 et 226-18-1 du code pénal.

Jusqu'à 300 000 € d'amende


Sanction prononcée par la CNIL, prévue par l'article 47 de la loi informatique et libertés modifiée.

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

Se mettre en conformité avec la CNIL. Quel est le rôle de l'audit ? | Denis JACOPINI



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

	<h2>Se mettre en conformité avec la CNIL. Quel est le rôle de l'audit ?</h2>
---	--

Depuis le 6 janvier 1978, les établissements public ou privés, les associations, les entreprises etc. doivent se mettre en conformité avec la Loi Informatique et Libertés. Un règlement européen entrant dans quelques mois en vigueur risquant de responsabiliser et sanctionner bien plus lourdement les concernés, il nous semblait important de vous détailler les étapes indispensables pour se mettre en conformité avec la CNIL.

Art. 226-16 de la Loi Informatique et Libertés

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés.

Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données, l'**#audit CNIL**, indépendant de la démarche de contrôle de la CNIL.

> Comment se passe un contrôle de la CNIL

Une fois cet **audit CNIL** réalisé, l'établissement connaissant enfin les actions qu'il doit mener va pouvoir prévoir deux actions de formation entrant dans notre cursus :

Se mettre en conformité avec la CNIL, mode d'emploi

- sensibiliser le personnel de l'établissement en lui expliquant la raison d'une démarche de mise en conformité CNIL et le comportement qu'il devra adopter pour favoriser cette action ;
 - former le futur correspondant CNIL (CIL) à devenir autonome en lui inculquant :
 - les notions clés et grands principes de la loi informatique et libertés ;
 - les principes de base en matière de sécurité des systèmes d'information ;
 - le traitement des demandes et les modalités d'instruction d'une plainte ;
 - les contrôles et les procédures de sanction de la CNIL
- La mise en application de la mise en conformité sur des cas concrets sur le système informatique de votre entreprise.

Au terme de ces démarches, un nouvel **audit CNIL** peut être réalisé afin de vérifier la conservation de la conformité dans le temps.



Intéressé par une démarche de mise en conformité avec la CNIL ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

Notre métier : Denis JACOPINI est Expert indépendant, Expert judiciaire en Informatique spécialisé en protection des données personnelles. Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapports d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Nous pouvons également 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 ; (Auteurs de la DITEP-EPIC 2011 et)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

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



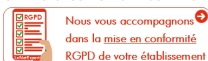
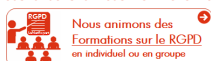
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

[block id="24761" title="Pied de page HAUT"]

Sources : Denis JACOPINI

<https://www.cnil.fr/fr/comment-se-passe-un-contrôle-de-la-cnil>

Mise en place d'un système de vote électronique, quelques conseils | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
<input type="checkbox"/>	Mise en place d'un système de vote électronique, quelques conseils				

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que tout système de vote électronique doit faire l'objet d'une expertise indépendante.

Le vote électronique, souvent via internet, connaît un développement important depuis plusieurs années, notamment pour les élections professionnelles au sein des entreprises.

La mise en place des traitements de données personnelles nécessaires au vote doit veiller à garantir la protection de la vie privée des électeurs, notamment quand il s'agit d'élections syndicales ou politiques.

La CNIL souligne que le recours à de tels systèmes doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin (sauf pour les scrutins publics), le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l'élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Les mesures de sécurité sont donc essentielles pour un succès des opérations de vote mais mettent en œuvre des mesures compliquées, comme par exemple l'utilisation de procédés cryptographiques pour le scellement et le chiffrement.

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que **tout système de vote électronique doit faire l'objet d'une expertise indépendante.**

Par ailleurs, l'article R2314-12 du Code du Travail créé par Décret n°2008-244 du 7 mars 2008 – art. (V) fixe très clairement que préalablement à sa mise en place ou à toute modification substantielle de sa conception, **un système de vote électronique est soumis à une expertise indépendante.** Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Information complémentaire : Les articles R2314-8 à 21 et R2324-4 à 17 du Code du Travail indiquent de manière plus générale les modalités du vote électronique lors du scrutin électoral de l'élection des délégués du personnel et des délégués du personnel au comité d'entreprise.

Ces dispositions ont été complétées par la délibération 2010-371 de la CNIL du 21 octobre 2010 portant adoption d'une

recommandation relative à la sécurité des systèmes de vote électronique.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des mesures décrites dans la présente délibération et notamment sur :

- le code source du logiciel y compris dans le cas de l'utilisation d'un logiciel libre,
- les mécanismes de scellement utilisés aux différentes étapes du scrutin (voir ci-après),
- le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
- les échanges réseau,
- les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur.

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

- Être un informaticien spécialisé dans la sécurité ;
- Ne pas avoir d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d'utiliser la solution de vote ;
- Posséder une expérience dans l'analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d'au moins deux prestataires différents ;
- Avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d'expertise doit être remis au responsable de

traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondants à la première version et aux évolutions substantielles de la solution de vote mise en place.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

L'expert doit fournir un moyen technique permettant de vérifier a posteriori que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise.

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises

L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

**Vous souhaitez organiser des élections
par voie électronique ?
Cliquez ici pour une demande de chiffrage
d'Expertise**



Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solutions de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

<http://www.cnil.fr/les-themes/vie-citoyenne/vote-electronique/>
<http://www.cnil.fr/documentation/deliberations/deliberation/de-lib/249/>

<http://infosdroits.fr/la-cnil-sanctionne-un-employeur-pour-defaut-de-securite-du-vote-electronique-pendant-une-election-professionnelle/>

Quelques exemples de sanctions et condamnations prononcées par la CNIL | Denis JACOPINI



Quelques sanctions CNIL prononcées auprès de sociétés commerciales

Quelques sanctions CNIL prononcées auprès de sociétés commerciales

- Société JEAN MARC PHILIPPE (DELIBERATION n°2009-201 du 16 avril 2009) : 10 000 euros d'amende pour avoir installé une vidéosurveillance permanente des salariés (COMMERCE VÊTEMENTS MAGASIN + SITE EN LIGNE PARIS)
En outre, le directeur général de la société JEAN MARC PHILIPPE s'étant opposé au contrôle de la CNIL, a été condamné par le Tribunal correctionnel de Paris à une peine d'amende de 5 000 euros pour délit d'entrave.
- DirectAnnonces : 40 000 euros d'amende pour pratiques déloyales Cette société est spécialisée dans la compilation d'annonces immobilières de particuliers sur internet pour revente à des professionnels (pratique jugée déloyale puisqu'elle se faisait à l'insu des personnes). (ANNONCES IMMOBILIERES PARIS)
- CDISCOUNT (30.000 € d'amende) et ISOTHERM (30.000 € d'amende) pour démarchage commercial par courriel et

téléphone abusif. Sanctions prononcées en novembre 2008 et rendues publiques en juin 2009. Ces deux sociétés ne prenaient pas en compte efficacement les demandes de désinscription des personnes ne souhaitant plus être démarchées alors que la loi informatique et libertés prévoit un droit d'opposition à la prospection commerciale. (MAGASIN EN LIGNE BORDEAUX)

- KEOLIS RENNES : avertissement public pour le passe Korrigo de Rennes (prononcé le 20 janvier 2009 et rendu public le 17 juin 2009). Un contrôle sur place a souligné de véritables obstacles pour souscrire un passe anonyme. (TRANSPORT PUBLIC DE VOYAGEURS RENNES)
- Entrepaticuliers.com : Par décision du 20 mai 2008, la CNIL, a prononcé un avertissement à l'égard de la société en raison de plusieurs manquements à la loi informatique et libertés, dont des défauts de sécurité. Information rendue publique le 17 novembre 2008. (ANNONCES IMMOBILIERES LEVALLOSIS PERET)
- Société Leclerc ARCYDIS SA : 30 000 € d'amende + Publication de la sanction sur son site internet et sur la base Légifrance – juillet 2008 (CENTRE LECLERC BOIS D'ARCY 78390)
- Société Neuf Cegetel : 7 000 € d'amende + Publication de la sanction sur son site internet et sur la base Légifrance – juin 2008 (OPERATEUR TELEPHONIQUE 92)
- Société VPC KHADR : 5 000 € d'amende + Publication de la sanction dans le quotidien La Nouvelle République du Centre Ouest – février 2008 (VENTE DE MOBILIE REN LIGNE ARGENTON SUR CREUSE 36)*****
- SERVICE INNOVATION GROUP France : Société spécialisée dans la force de vente et le marketing : 40 000 € d'amende – décembre 2007 (78140 VELIZY VILLACOUBLAY)
- Société JPSM (nom commercial « Stock Premium ») : 5000 € d'amende – novembre 2007 (BOUTIQUE VÊTEMENTS NANCY)
- Société B&M : Société de Conseils – 10 000 € d'amende – octobre 2007 (LA RICHE 37)

- Cabinet d'enquêtes privées (non public) : Recherche de débiteurs – 50 000 € d'amende – juin 2007
- FRDT – Entreprise spécialisée dans l'immobilier : 15 000 € d'amende – mai 2007 (TOULON 83)
- Studio Replay – Entreprise de vente à distance : 10 000 € d'amende – mars 2007
- Cabinet de recouvrement de créances : 5 000 € d'amende – mars 2007
- BANQUE DES ANTILLES FRANCAISES : 30 000 € d'amende – mars 2007 (PARIS)
- Opérateur télécom (Non Public) : 10 000 € d'amende – mars 2007
- Entreprise de vente à distance (Non public) : 5 000 € d'amende – déc. 2006
- La société Tyco HealthCare (Matériel médical) : 30 000 € d'amende – déc. 2006. (PLAISIR 78)
- Deux enseignes spécialisées dans la vente de fenêtres (Non public) : 60 000 € d'amendes – Déc. 2006
- Le Crédit Agricole Centre France : 20 000 € d'amende – Nov. 2006
- Etablissement financier (Non Public) : 1 000 € d'amende – Sept. 2006
- Entreprise d'électricité (non public) : 1 500 € d'amende – Sept. 2006
- Expertise financière Cabinet de conseil : 500 € d'amende – Sept. 2006
- Prestataire internet (Non Public) : 300 € d'amende - Sept. 2006

- Etude d'huissiers de justice (Non Public) : 5000 € d'amende- Juin 2006
- LCL (anciennement Le Crédit Lyonnais) : 45 000 € d'amende – Juin 2006

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

Mise en place d'un système de vidéosurveillance – Rappel des règles | Denis JACOPINI



La Commission nationale de l'informatique et des libertés (Cnil) a de nouveau rappelé qu'un dispositif de vidéosurveillance ne peut être disproportionné par rapport à l'objectif de sécurité recherché, et ne peut intervenir que dans le respect de la vie privée des salariés.

Rappelons que pour être licite le dispositif de surveillance mis en place doit avoir pour objectif la sécurité des biens et des personnes.

À ce titre, seuls les endroits considérés comme « à risque » doivent faire l'objet d'une surveillance.

Le dispositif ne doit pas être détourné de sa finalité, et ne peut donc aboutir à surveiller les horaires de travail.

Par ailleurs, la surveillance ne peut apporter aux libertés individuelles et collectives « de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché » (C. trav., art. L. 1121-1).

Ainsi, le dispositif mis en place ne doit pas aboutir à une surveillance permanente des salariés (sauf cas exceptionnel justifié par une exposition particulière à un risque). Enfin, la mise en place du dispositif doit faire l'objet d'une information et consultation des représentants du personnel, et d'une information individuelle des salariés.

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

Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT RGD CYBER MISES EN CONFORMITE</p>	 <p>LE NET EXPERT SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
<div>  <p>Denis JACOPINI</p> <p>VOUS INFORME</p> </div> <div> <p>Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi</p> </div>					

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

Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés.- Que se cache derrière cette loi ?

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

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

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



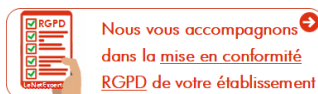
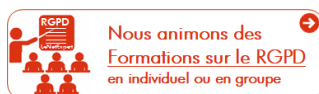
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

[block id="24761" title="Pied de page HAUT"]

Les conseils pour faire connaître son site Internet et les outils pour Webmasters | Denis JACOPINI



AUDIT DE CONTENU DE SITES INTERNET

Google Webmaster Tools

Google Webmaster Tools est un outil pertinent et facile d'utilisation pour les éditeurs qui cherchent à optimiser le référencement naturel de leurs pages web. De l'exploration des pages par les robots, à l'analyse des mots-clés, en passant par la qualité/quantité des liens retours et le positionnement des pages : il analyse de nombreux paramètres SEO décisifs pour améliorer la visibilité d'un site web sur Google.

Screaming Frog

Disponible pour Mac et PC, Screaming Frog audite un site, ses liens, images, CSS et scripts pour en ressortir des indicateurs utiles à l'indexation et au SEO. Au-delà des erreurs HTTP rencontrées lors du crawl, l'outil va également faire remonter les balises Title, H1 ou H2 manquantes, dupliquées ou trop longues. L'ancre des liens rencontrés est précisée, tout comme leur éventuel attribut *nofollow*.

Bing pour Webmasters

Certes, « Bing Webmaster » est plus intéressant pour des sites positionnés dans des pays où Bing a une part de marché significative, mais même en France, il a plusieurs intérêts. Puisqu'il peut par exemple auditer un site, ou retrouver des liens pointant vers n'importe quelle page.

MajesticSEO

MajesticSEO analyse des liens entrants de n'importe quel site web. Ses indicateurs maison, le score de citation (« Citation Flow ») et le score de crédibilité (« Trust Flow »), sont souvent cités par les SEO pour évaluer la qualité d'un site web et de ses liens sortants. Bâti sur des centaines de milliards d'URL crawlées, le service est régulièrement actualisé, et propose souvent de nouvelles fonctionnalités.

Open Site Explorer

Open Site Explorer ou OSE est un outil est bien connu pour ses analyses de backlinks et de l'autorité de leur origine. OSE peut être utilisé gratuitement, mais en version bridée. L'analyse complète, et certains indicateurs, comme ceux concernant les partages sociaux d'une page, sont cependant réservés à la version payante.

Moz

Certains outils de cette suite sont gratuits, comme la météo des pages de résultats de Google.com ou l'analyse des comptes Twitter. Mais les plus utiles (analyse de mot clé, crawl et audit de site, suivi de position...) nécessitent un abonnement, facturé à partir de 99 dollars par mois.

AUDIT DE TEST DE SITE INTERNET

WebPageTest – Mesure de vitesse d'ouverture des pages

FAIRE CONNAITRE SON SITE INTERNET SUR LES RESEAUX SOCIAUX

15/04/2014 26 idées pour obtenir plus d'abonnés Google+

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

Références :

28/02/2014

<http://www.journaldunet.com/solutions/seo-referencement/seo-les-meilleurs-outils/google-webmaster-tools.shtml>

27/02/2014

<http://ecommerce-live.net/event/nouvelle-strategie-de-referencement-en-2014-quand-le-virtuel-rencontre-le-reel-3/>

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

Emailing – Rappel des règles d'utilisation des données personnelles dans le cas de la prospection | Denis JACOPINI



Dans le cadre de vos activités, vous pouvez être amenés à contacter par E-mail des personnes.
Quelles sont les règles à respecter ?

LA PROSPECTION PAR COURRIER ÉLECTRONIQUE Pour les particuliers (B to C) :

Le principe dans l'emailing : pas de message commercial sans accord préalable du destinataire

La publicité par courrier électronique est possible à condition que les personnes aient explicitement donné leur accord pour être démarchées, au moment de la collecte de leur adresse électronique.

Deux exceptions à ce principe :

- si la personne prospectée est déjà cliente de l'entreprise et si la prospection concerne des produits ou services analogues à ceux déjà fournis par l'entreprise.
- si la prospection n'est pas de nature commerciale (caritative par exemple)

Dans ces deux cas, la personne doit, au moment de la collecte de son adresse de messagerie être informée que son adresse électronique sera utilisée à des fins de prospection, être en mesure de s'opposer à cette utilisation de manière simple et gratuite.

LA PROSPECTION PAR COURRIER ÉLECTRONIQUE Pour les professionnels (B to B) :

Le principe : information préalable et droit d'opposition

La personne doit, au moment de la collecte de son adresse de messagerie être informée que son adresse électronique sera utilisée à des fins de prospection, être en mesure de s'opposer à cette utilisation de manière simple et gratuite.

L'objet de la sollicitation doit être en rapport avec la profession de la personne démarchée (exemple : message présentant les mérites d'un logiciel à paul.toto@nomdelasociété , directeur informatique.)

Les adresses professionnelles génériques de type (info@nomsociete.fr, contact@nomsociete.fr, commande@nomsociete.fr) sont des coordonnées de personnes morales. Elles ne sont pas soumises aux principes du consentement et du droit d'opposition.

DANS TOUS LES CAS :

Chaque message électronique doit obligatoirement:

- préciser l'identité de l'annonceur,
- proposer un moyen simple de s'opposer à la réception de nouvelles sollicitations (par exemple lien pour se désinscrire à la fin du message).

La CNIL recommande que le consentement préalable ou le droit d'opposition soit recueilli par le biais d'une case à cocher. L'utilisation d'une case pré-cochée est à proscrire car contraire à la loi.

LÉGISLATION APPLICABLE

Article L.34-5 du Code des postes et des communications électroniques

Article L.121-20-5 du Code de la consommation.

RÉFÉRENCES UTILES

Code de déontologie de la communication directe électronique du SNCD (Syndicat National de la Communication Directe)

Code Déontologique du e-commerce et de la vente à distance du FEVAD (Fédération du e-commerce et de la Vente à Distance)

Le rapport relatif à l'Opération boîte à spam de la CNIL

SANCTIONS

Amende de 750 € par message expédié

Contravention de la 4e classe prévue par l'article R.10-1 du code des postes et des communications électroniques.

5 ans emprisonnement et 300 000 € amende

Délit prévu par les articles 226-18 et 226-18-1 du code pénal.

Jusqu'à 300 000 € d'amende

Sanction prononcée par la CNIL, prévue par l'article 47 de la loi informatique et libertés modifiée.

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

**Pourquoi supprimer vos
données personnelles si vous
rendez votre ordinateur
professionnel à votre
employeur ?**



Pourquoi supprimer
vos données
personnelles si
vous rendez votre
ordinateur
professionnel à
votre employeur ?

Ne pas effacer ses données personnelles sur son ordinateur de fonction est-il dommageable (risque d'accès à nos données personnelles, vol d'identité ou accès frauduleux etc...)? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :

- Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix ;
- Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox... ;
- Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité. Même si l'article 226-4 du code pénal complété par la loi LOPPSI du 14 mars 2011 d'un article 226-4-1, l'usurpation d'identité numérique est un délit puni de deux ans d'emprisonnement et de 20 000 euros d'amende, il sera fastidieux d'une part pour vous, de prouver que vous n'êtes pas le véritable auteur des faits reprochés, et difficile pour les enquêteurs de retrouver le véritable auteur des faits.

Ne pas effacer ses données personnelles sur l'ordinateur que l'on rend, donne, vend, c'est laisser l'opportunité à un inconnu de fouiller dans vos papiers, violer votre intimité et cambrioler votre vie.

Pire ! vous connaissez bien le donataire de votre matériel et vous savez qu'il n'y a aucun risque qu'il ait des intentions répréhensibles. Mais êtes vous certain qu'il sera aussi prudent que vous avec son matériel ?

Êtes-vous prêt à prendre des risques s'il perdait ce matériel ?

Dormiriez-vous tranquille si vous imaginiez que votre ancien ordinateur est actuellement sous l'emprise d'un pirate informatique prêt à tout pour tricher, voler et violer en utilisant votre identité ?

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

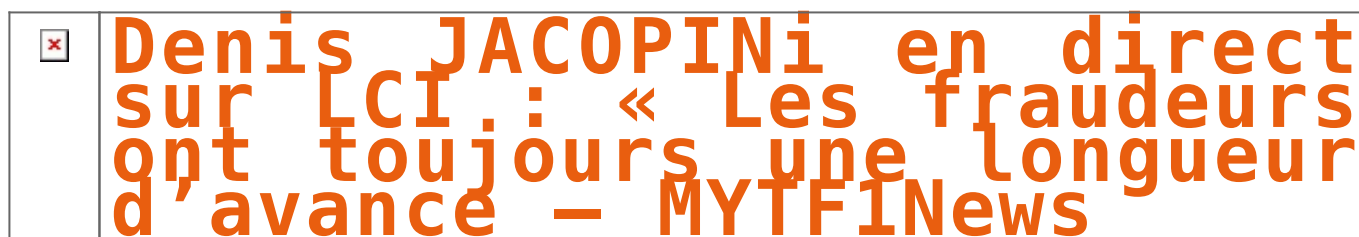


[Contactez-nous](#)

Réagissez à cet article

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

Denis JACOPINI en direct sur LCI : « Les fraudeurs ont toujours une longueur d'avance – MYTF1News | Denis JACOPINI



Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.

En direct sur LCI avec Serge Maître Maître, président de l'AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent sur les techniques des cybercriminels pour vous pirater votre CB.



<http://lci.tf1.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html>



Réagissez à cet article

Source : *Cartes bancaires : « Les fraudeurs ont toujours une longueur d'avance » – Société – MYTF1News*