Vidéoprotection / vidéosurveillance : le public doit-il être informé qu'il est filmé ? | Denis JACOPINI

Vidéoprotection / vidéosurveillance : le public doit-il être informé qu'il est filmé ?

Les personnes filmées dans un espace public (rue, administration, gare, centre commercial, banque etc.) doivent en être informées, au moyen de panneaux affichés de façon visible comportant :
• Un pictogramme représentant une caméra
• Le nom ou la qualité et le numéro de téléphone du responsable
Ces panneaux doivent être affichés en permanence dans les lieux concernés et doivent être compréhensibles par tous les publics.

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. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source :
https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=514319E089C032799DD14161D6197C4C?name=Vid%C3%A9oprotection%2Fvid%C3%A9osurveillance+%3A+le+public+doit-il+%C3%AAtre+inform%C3%A9+qu%27il+est+film%C3%A9+%3F&id=409

Données personnelles, e-commerce et CGV. Par Sarah

Garcia, Avocate. | Denis JACOPINI

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

Données personnelles, e-commerce et CGV

Considérées comme le socle de la relation contractuelle, les #conditions générales de vente (CGV) désignent l'ensemble des clauses qui constituent l'offre émise par un vendeur professionnel à destination des acquéreurs potentiels de ses produits.

Avec le développement du commerce en ligne, la protection des données personnelles devient un enjeu important en termes d'image de l'entreprise, mais aussi et surtout en termes de confiance que l'utilisateur a dans le site. Comme le souligne la présidente de la CNIL, « la protection des données personnelles est un avantage concurrentiel pour les entreprises ».
La protection des données personnelles est au cœur du fonctionnement du site e-commerce, à travers le recueil d'informations relatives à l'identification des personnes (nom, adresse, numéro de téléphone, numéro de carte bancaire…)
La loi informatique et libertés du 6 janvier 1978 modifiée assure à travers une série de règles la protection de ces données personnelles. La création et le traitement de données à caractère personnel sont soumis à des obligations destinées à protéger la vie privée des personnes des prospects et les libertés individuelles.
Sans être exhaustif, nous allons aborder les règles qu'impose la CNIL dans le cadre du respect des #droits des clients, la durée de conservation de ces données personnelles, les règles applicables dans le cadre de la prospection commerciale, qui sont autant de domaines qui touchent à la protection des données personnelles.

1. Le respect des droits des clients
Les conditions générales de vente lorsqu'elles recueillent des données personnelles doivent mentionner les droits des personnes dont les données sont recueillies.
Les CGV doivent donc mentionner les procédés mis en œuvre par le site de e-commerce afin de garantir les droits de ces personnes.

Le droit d'être préalablement informé (article 32 de la loi Informatique et Libertés).
Le droit de consentir (article 7 de la loi informatique et libertés).
Le #droit d'accès (article 39, I, 4° de la loi informatique et libertés)
Le #droit de rectification (article 40 de la loi informatique et libertés)
Le #droit d'opposition (article 38 de la loi informatique et libertés).
En règle générale, une clause de ces conditions générales doit renvoyer aux conditions de mise en œuvre. Il est également possible de rédiger séparément une #politique de protection des données personnelles sur le site.

2. La #durée de conservation des données
La loi informatique et libertés prévoit qu'un traitement ne peut porter que sur des données à caractère personnel qui sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées (article 6, 5°).

En pratique, la CNIL recommande de respecter les durées suivantes :
Concernant les éléments d'identité des clients habituels et occasionnels : 5 ans à compter de la clôture du compte ou de la relation commerciale.
Concernant les documents et informations relatifs aux opérations faites par les clients. Il peut s'agir du dépôt, du retrait, des virements, des prélèvements, des opérations concernant les cartes. La durée de conservation est de 5 ans à compter de l'exécution de l'opération.
Toutes ces informations peuvent figurer aussi bien dans les conditions générales de vente que dans un document intitulé « politique de protection des données personnelles » et mis à la disposition des utilisateurs sur le site internet.

3. Le #recueil du consentement dans le cadre de la prospection commerciale et du parrainage
Cette prospection commerciale se fait généralement par voie électronique, appel téléphonique ou centre d'appel.
Le recueil du consentement du prospect est important. Le site d'e-commerce peut en effet s'exposer à payer une amende ou une peine d'emprisonnement.

En cas de prospections commerciales effectuées par voie postale, ou par appel téléphonique depuis un centre d'appel, l'envoi de publicité par voie postale est possible sous réserve que la personne soit, au moment de la collecte de ses coordonnées informée de leur utilisation à des fins de prospection et en mesure de s'opposer à cette utilisation de manière simple et gratuite. Telle est la préconisation de la CNIL. C'est le système de l'op out.

En matière de publicité par voie électronique, le principe en la matière est de recueillir l'accord préalable du destinataire. C'est le système de l'op in. La CNIL a ainsi récemment condamnée la Société Prisma Media a payé une amende de 15.000 euros pour envoi sans le consentement des prospects de lettres d'information électronique contenant de la prospection [1]

En effet, la CNIL subordonne l'envoi de publicité à des prospects par la voie électronique à un consentement. Dans la pratique, ce consentement doit être matérialisé par une case à cocher.

Toutefois des exceptions demeurent :
Si la personne prospectée est déjà cliente de l'entreprise et si la prospection concerne des produits ou des services analogues à ceux déjà fournis par l'entreprise.
Si la prospection n'est pas de nature commerciale.

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.

En ce qui concerne les professionnels, le principe est celui de l'information préalable et le droit d'opposition. Il faut ainsi que la personne soit informée que son adresse électronique est utilisée à des fins de prospection commerciale, et être en mesure de s'opposer à cette utilisation de manière simple et gratuite.

Le consentement doit être recueilli sans aucune ambiguïté. Ainsi, l'utilisation d'une case pré-cochée est à proscrire.
Le non-respect de ces dispositions est sanctionné par une amende de 750 euros par message expédié et 5 ans d'emprisonnement et 300.000 euros d'amende.

4. Le parrainage et les jeux concours
La recherche de nouveaux prospects, le site e-commerce peut organiser un système de parrainage ou des jeux concours. Ils ne sont pas interdits, mais il est nécessaire de respecter la protection des données personnelles.

a. Le parrainage
Qu'est-ce que le parrainage ? Il a pour objet de demander à une personne de renseigner les coordonnés d'un tiers qui peut être intéressé par une offre commerciale.
Comment respecter le droit relatif à la protection des données personnelles ? La CNIL précise que le destinataire de l'offre doit connaître l'identité de son parrain lorsqu'il est contacté par l'entreprise. Ensuite, les données du parrainé ne peuvent être utilisées qu'une seule fois pour lui adresser l'offre commerciale, l'article de presse ou l'annonce suggéré par le parrain. Enfin, l'entreprise ne pourra conserver les données du parrainé pour lui adresser d'autres messages que si elle a obtenu son consentement exprès.
Tout comme l'organisation des jeux concours, le parrainage ne doit pas être dilué dans les conditions générales de vente.

b. Les jeux concours
L'organisation des jeux concours est attractive et peut permettre de capter la clientèle. L'internaute doit pouvoir participer à un jeu concours sans être obligé de recevoir de la prospection.
La CNIL précise que les informations recueillies concernant le joueur ne peuvent être utilisées que dans le cadre du jeu et la remise du lot. Les coordonnées électroniques du participant ne peuvent pas être utilisées à des fins publicitaires, sauf consentement exprès de sa part.
Il est essentiel que le responsable du fichier reprenne les mentions de la loi « informatique et libertés » sur le formulaire de participation au jeu-concours. Il doit être remis au participant le règlement du jeu concours dans lequel figurera une rubrique « vie privée ».
La CNIL précise par ailleurs que le consentement préalable doit être recueilli par un moyen simple et gratuit, comme une case à cocher par exemple. Pour que le consentement soit valide, la case ne doit pas être « pré-cochée ».

5. La #gestion des cookies
a. Le cadre juridique applicable.
Le législateur européen a posé le principe (directive 2009/136/CE) d'un consentement préalable de l'utilisateur avant le stockage d'informations sur son équipement ou l'accès à des informations déjà stockées. Ce consentement préalable n'est pas nécessaire si les actions sont strictement nécessaires pour la délivrance d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

b. Quels sont les cookies concernés et nécessitant un consentement préalable ?
Sont concernés les traceurs déposés et lus par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisé tels qu'un ordinateur, un smartphone, une liseuse numérique et une console de jeux vidéos connectée à Internet. Il s'agit par exemple de cookies http, ou de cookie flash…
Ces obligations sont requises que les cookies collectent des données à caractère personnel ou non.
Pour les cookies nécessitant une information préalable et une demande de consentement, on peut notamment citer ceux liés aux opérations relatives à la publicité ciblée ; certains cookies de mesure d'audience ou encore les cookies des réseaux sociaux engendrés notamment par leurs boutons de partage lorsqu'ils collectent des données personnelles sans consentement des personnes concernées. Cette liste n'est pas exhaustive.
Il convient de souligner que le cookie de mesure d'audience est exempté dans certains cas de consentement de l'internaute.

c. La mise en conformité du site
L'obligation est donc double pour le site : une information préalable et un consentement préalable.
En règle générale, l'internaute doit avoir un affichage d'un bandeau d'information sur la première page du site visité.

Un modèle pourrait être libellé comme suit :
« En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de [Cookies ou autres traceurs] pour vous proposer [par exemple, des publicités ciblées adaptés à vos centres d'intérêts] et (par exemple, réaliser des statistiques de visites]. »
Pour en savoir plus et paramétrer les traceurs : Source la CNIL.

En définitive, la politique de protection des données personnelles est un élément que le site e-commerce doit prendre en compte dans la rédaction des conditions générales de vente et dans la gestion de son site. Éléments essentiels et incontournables, les sites de e-commerce doivent intégrer cette réalité. Car un respect de ces obligations légales est aussi un outil marketing pour le développement de ces sites.

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

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : http://www.village-justice.com/articles/Donnees-personnelles-commerce-CGV,20003.html
Par Sarah Garcia, Avocate

Qui peut le consulter le fichier des impayés de la téléphonie mobile Préventel ? | Denis JACOPINI

Qui peut le consulter le fichier des impayés de la téléphonie mobile Préventel ?

Le fichier peut être consulté par le GIE Preventel et par les les services des membres du GIE Préventel chargés de la gestion des abonnements et des recouvrements.
Le fichier est consulté pour chaque nouvelle demande d'abonnement mobile par les services chargés de l'ouverture de ligne.
Les vendeurs en boutique n'ont pas directement accès au fichier PREVENTEL.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=4A1F561B7B702AD8312BAF603CB6F9F0?name=Pr%C3%A9ventel+(fichier+des+impay%C3%A9s+de+la+t%C3%A9l%C3%A9phonie+mobile)+%3A+qui+peut+le+consulter+%3F&id=378

Qu'est-ce que le registre RGPD ?

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

Qu'est-ce que le registre RGPD ?

Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.

Document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :
• les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
• les catégories de données traitées,
• à quoi servent ces données (ce que vous en faites),
• qui accède aux données et à qui elles sont communiquées,
• combien de temps vous les conservez,
• et comment elles sont sécurisées.
Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de votre conformité au RGPD. Il vous permet de documenter vos traitements de données et de vous poser les bonnes questions : ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.
Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle vous permettra d'en déduire un plan d'action de mise en conformité de vos traitements aux règles de protection des données.

Qui est concerné ?

L'obligation de tenir un registre des traitements **concerne tous les organismes, publics comme privés et quelle que soit leur taille,** dès lors qu'ils traitent des données personnelles.

Dispositions pour les organismes de moins de 250 salariés

Les entreprises de moins de 250 salariés bénéficient d'une dérogation en ce qui concerne la tenue de registres. **Ils doivent inscrire au registre les seuls traitements de données suivants** :
• les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
• les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.)
• les traitements qui portent sur des données sensibles (exemple : données de santé, infractions, etc.).
En pratique, cette dérogation est donc limitée à des cas très particuliers de traitements, mis en œuvre de manière occasionnelle et non routinière, comme par exemple une campagne de communication à l'occasion de l'ouverture d'un nouvel établissement, sous réserve que ces traitements ne soulèvent aucun risque pour les personnes concernées. En cas de doute sur l'application de cette dérogation à un traitement, la CNIL vous recommande de l'intégrer dans votre registre.

Un registre spécifique pour les activités de sous-traitance des données personnelles

Les organismes qui traitent des données personnelles **pour le compte d'un autre organisme**(les sous-traitants comme, par exemple, des prestataires de services informatiques ou des agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients) doivent également tenir un registre de leurs activités de sous-traitant impliquant le traitement de données.
Pour plus de précisions : voir le guide RGPD pour les sous-traitants

---

Que contient le registre ?

L'article 30 du RGPD prévoit des obligations spécifiques pour le registre du responsable de traitement de données personnelles et pour le registre du sous-traitant. Si votre organisme agit à la fois en tant que sous-traitant et responsable de traitement, votre registre doit donc clairement distinguer les deux catégories d'activités.
En pratique, dans cette hypothèse, la CNIL vous recommande de tenir 2 registres :
1. un pour les traitements de données personnelles dont vous êtes vous-même responsable,
2. un autre pour les traitements que vous opérez, en tant que sous-traitant, pour le compte de vos clients.
[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

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

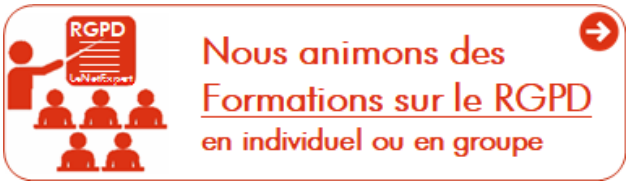
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

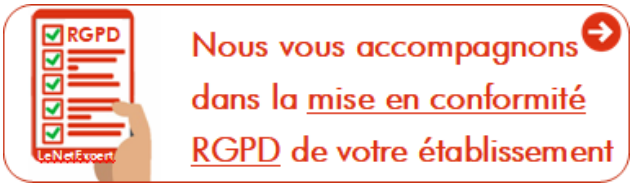
Contactez-nous

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source : *Le registre des activités de traitement*

Que faire pour limiter les risques d’usurpation d’identité numérique ? | Denis JACOPINI

Que faire pour limiter les risques d’usurpation d’identité numérique ?

Que faire pour limiter les risques d’usurpation d’identité numérique ?

• Surveiller la bonne réception des factures courantes et du courrier en général ;
• Mettre des signes de sécurité sur toutes les copies de documents que vous envoyez à des tiers ;
• Ne jamais accepter de laisser vos documents d’identité ou de voyage à des hôtesses d’accueil ou des agents de sécurité en échange d’un badge, y compris dans les locaux de l’administration. C’est illégal ;
• Demandez des garanties à des commerçants qui traitent vos données (concessionnaires automobiles, notaires, agences immobilières, etc.) ;
• Examiner soigneusement vos relevés de compte bancaire pour détecter rapidement la moindre anomalie ;
• Détruire systématiquement avec un destructeur de documents (de préférence coupe croisée), les documents de l’assurance maladie, les chèques annulés, les impressions comportant vos coordonnées ;
• Ne pas laisser son courrier à la portée d’indiscrets.
• Limiter le nombre de cartes de crédit ou de paiement, les signer dès réception, ne jamais les prêter ni communiquer leurs codes, annuler toute carte de crédit inactive ;
• Examiner soigneusement ses relevés de compte pour détecter rapidement la moindre anomalie ;
• Avertir immédiatement dans l’ordre : 1- les forces de police en déposant une plainte, 2- les organismes concernés en cas de vol de carte de paiement ;
• Avertir immédiatement les organismes concernés en cas de perte de carte de paiement ;
• Détruire systématiquement avec un destructeur de documents (de préférence coupe croisée) les chèques annulés, les reçus de carte de crédit et les justificatifs de paiement ;
• Ne jamais conserver le code confidentiel d’une carte, un mot de passe ou un numéro d’assurance sociale dans son portefeuille ;
• Utiliser une adresse email « informelle jetable » pour remplir toutes les demandes d’inscriptions à des comptes divers ;
• Toujours cocher la case « je refuse que mes données personnelles figurent dans le fichier informatisé de la société ».

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l’Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.globalsecuritymag.fr/Usurpation-d-identite-en-2015,20151014,56659.html
par Emmanuelle Lamandé

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 Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

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

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 sevra 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 ?

Contatez-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 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.

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, 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

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.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84

Datadock Organisme validé et référencé

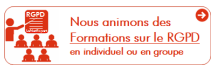
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

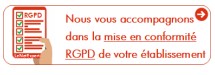
Contactez-nous

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-controle-de-la-cnil

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 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)
- Entreparticuliers.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)

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale | Denis JACOPINI

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale.
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. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l’hygiène informatique.
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.aide.cnil.fr/selfcnil/site/template.do?name=D%C3%A9clarer%C2%A0%C3%A0+la+CNIL%2C+c%27est+obligatoire+%3F&id=335

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)