Se mettre en conformité avec la CNIL – Oui mais comment ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	**Dossier du moi de juille 2014 :Se mettre en conformité avec la CNIL – Oui mais comment ?** Encore plus fort que la peur du gendarme, la peur d'avoir mauvaise réputation est la principale crainte des entreprises concernées par des actes illicites (C'est ce qui ressort d'une étude de PWC). Des années pour la construire, une fraction de seconde pour la salir; Et si votre manque de respect des données personnelles de vos clients vous rattrapait..				

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.

Les contrôles de la CNIL ne font que commencer. Alors que la loi n° 2014-344 du 17 mars 2014 donne le pouvoir à la CNIL

d’effectuer des contrôles et dresser des P.V. à distance (à la manière des forces de l’ordre qui verbalisent les infractions à partir d’images issues de vidéo-surveillance) et qu’un projet de règlement européen propose d’augmenter le montant des amendes et d’obliger toute structure victime d’une faille de sécurité informatique, de le déclarer à la CNIL et à toutes les personnes concernées par le préjudice,

SE METTRE EN CONFORMITE AVEC LA CNIL – OUI MAIS COMMENT ?

Force est de constater, au fil des conférences régulièrement animées par Denis Jacopini, sur le thème des « obligations des chefs d’entreprises face aux nouveaux usages de l’informatique », que les entreprises partent de très loin et ont beaucoup de travail à faire pour se mettre en règle ». « Elles sont toutes concernées mais quasiment aucune n’a encore entamé de démarche.

1°/ Présentation pédagogique

Depuis le début de l’année 2013, Denis Jacopini sillonne le sud de la France pour animer régulièrement des conférences.

Une conférence, « La responsabilité des Chefs d’entreprise face aux nouveaux usages de l’informatique » marque particulièrement les esprits par ce qui est appris sur les « obligations de CNIL ».

« Mais on ne nous a jamais rien dit ! » , « Alors depuis des années je suis dans l’illégalité ? », « Je ne peux pas m’en

occuper seul ! »

Telles sont quelques unes des observations faites par les invités en fin de présentation.

Tous semblent découvrir que chaque traitement de données personnelles doivent faire l'objet d'une déclaration auprès de la CNIL.

Certains pensaient, au lieu de déclarer simplement le traitement qui était effectué sur leurs données, qu'il était nécessaire d'envoyer l'ensemble de leurs données à la CNIL et, craignant de se les faire voler, ne faisaient aucune démarche.

Besoin d'un accompagnement pour vous mettre en conformité avec la CNIL ?

N'hésitez pas à nous contacter

2°/ La CNIL pour quoi faire ?

La conférence l'explique de manière très vivante et particulièrement pédagogique. Vous devez d'abord connaître le coté « BON » de la CNIL pour les consommateurs.

En effet, cette Autorité Administrative Indépendante a d'abord en charge de veiller à la protection des données personnelles.

Seriez-vous d'accord si, en tant que consommateur, chaque fois que vous déclinez votre identité à quelqu'un, que vous lui communiquez votre numéro de téléphone, votre numéro de Carte Bancaire, votre numéro de sécurité Sociale ou transmettiez un RIB, vous trouviez un accès ou une copie de ces informations librement sur Internet ?

Je présume que non ! et je pense même que vous seriez soulagé si une loi obligeait les destinataire de votre identité

numérique à la protéger des curieux…

Cette Loi existe, c'est la loi Informatique et Libertés du 6 janvier 1978 et la CNIL a pour mission de veillez à ce que chaque professionnel, association, collectivité etc. la respecte. Et pour sensibiliser tous ces organismes à la confidentialité (entre autre) que vous êtes en droit d'exiger, **la CNIL effectue de plus en plus de contrôles** et à ce titre, elle dispose notamment d'un pouvoir de contrôle et de sanction.

Besoin d'un accompagnement pour vous mettre en conformité avec la CNIL ?

N'hésitez pas à nous contacter

3°/ Que faut-il déclarer à la CNIL ?

Sont concernés par des déclarations à la CNIL, les traitements impliquant et contenant des données personnelles.

Qu'est ce qu'une donnée personnelle ?

Art. 2 de la loi « Informatique et libertés » » Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il

convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne « .

Quelques exemples de données pouvant être considérées comme données personnelles : Nom, prénom, adresse, fonction dans une entreprise, date de naissance, diplôme, appartenance religieuse, appartenance politique, informations sur un état mental, informations sur un état de santé, adresse IP, adresse e-mail, numéro téléphone, numéro SIREN.

Quelques exemples de données incontestablement personnelles : Numéro de sécurité sociale, numéro carte d'identité, numéro de permis de conduire, numéro de passeport, numéro d'immatriculation, numéro carte bancaire, informations biométriques (empreinte digitale, rétinienne, faciale, ADN)

Qu'est ce qu'un traitement de données personnelles ?

Art. 2 de la loi « Informatique et libertés » « Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction « .

Exemple de traitements professionnels pouvant être concernés :

Système de facturation, système de relation client ou de gestion commerciale, fichier d'adresses , application informatique, base contacts, autocommutateur, espaces numériques de travail, système d'enregistrement des conversations téléphoniques sur support numérique. Également toute procédure de télétransmission de données personnelles,

d’interconnexion, de consultation et ce quel que soit le moyen de télécommunication ainsi que toute application de cartes à puce.

Ne sont pas concernés par la loi, les traitements mis en œuvre pour l’exercice d’activités exclusivement personnelles (agendas électroniques, répertoires d’adresses personnelles, …) et les fichiers membres et donateurs des associations .

Ainsi, si nous vous écrivons que sont concernés par des déclarations à la CNIL, les traitements impliquant et contenant des données personnelles, vous savez mieux de quoi nous parlons.

Besoin d’un accompagnement pour vous mettre en conformité avec la CNIL ?

N’hésitez pas à nous contacter

4°/ Au delà des déclarations

Il ne suffit pas de seulement déclarer sont traitement de données personnelles pour être en règle (même si dans certains cas, plus rares, il est nécessaire non pas de procéder à une déclaration de traitement de données personnelles mais plutôt une demande d’autorisation de traitement de données personnelles ou une demande d’avis auprès de la CNIL).

En effet, les traitements sont toujours une résultante de collectes pour lesquelles certaines obligations d’informations sous formes de mentions légales doivent être scrupuleusement respectées.

Exemple de mention légale : *Système de traitement de données personnelles déclaré à la CNIL sous le n°xxx-xxxx Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à ……(Veuillez préciser le service et l'adresse). Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.*

Besoin d'un accompagnement pour vous mettre en conformité avec la CNIL ?

N'hésitez pas à nous contacter

5°/ Concrêtement

Pour vous mettre en conformité avec la CNIL, il vous suffit :

- d'identifier TOUS les traitements concernés par la Loi Informatique et Libertés,
- de contrôler s'il existe une réglementation spécifique à votre métier,
- d'appliquer les recommandations de la CNIL de la collecte au stockage,
- de déclarer chaque traitement à la CNIL ou déclarer un CIL (Correspondant Informatique et Libertés) qui tiendra

à jour un registre,

- de vérifier régulièrement le respect des traitements déclarés, l'évolution des traitements soumis à correction et la présence éventuelle de nouveaux traitements en fonction de l'évolution de la structure.

Besoin d'un accompagnement pour vous mettre en conformité avec la CNIL ?

N'hésitez pas à nous contacter

6°/ Sanctions concrètes

Dans cette affaire, un fichier client (contenant des données personnelles) a été cédé par une société à un individu, qui a ensuite cherché à faire annuler la vente. Après avoir été débouté en première instance et en appel, le cessionnaire a obtenu satisfaction devant la cour de Cassation et faisant valoir le fait que le fichier n'était ps déclaré à la CNIL et était donc illicite.

http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000027632440&fastReqId=1263965640&fastPos=1

Quelques exemples de sanctions et condamnations prononcées par la CNIL

http://www.lenetexpert.fr/quelques-exemples-sanctions-condamnations-prononcees-cnil/

Sanctions prononcées depuis l’entrée en vigueur de la loi relative au défenseur des droits

http://www.cnil.fr/linstitution/missions/sanctionner/les-sanctions-prononcees-par-la-cnil/c5545

Besoin d’un accompagnement pour vous mettre en conformité avec la CNIL ?

N’hésitez pas à nous contacter

7°/ Le projet de règlement européen en 3 minutes

https://www.youtube.com/watch?v=_aDlRghIZww##t=30

Besoin d’un accompagnement pour vous mettre en conformité avec la CNIL ?

N’hésitez pas à nous contacter

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

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

Contactez-nous

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

« *Mon objectif, vous assurer une démarche de mise en*

conformité validée par la CNIL. ».

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

Quelques articles sélectionnés par nos Experts :

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

Réagissez à cet article

Références :

http://www.cnil.fr/linstitution/actualite/article/article/un-pouvoir-dinvestigation-renforce-grace-aux-controles-en-ligne/
http://www.pwc.com/fr_CA/ca/risk/forensic-services/publications/pwc-economic-crime-survey-canadian-supplement-2014-02-fr.pdf
http://www.lenetexpert.fr/wp-content/uploads/2014/03/La-loi-informatique-et-Libertés-au-01.06.2013.pdf