RGPD : Que se passe t-il si le 25 mai 2018 nous n’avons pas terminé notre mise en conformité ?

	RGPD : Que se passe t-il si le 25 mai 2018 nous n’avons pas terminé notre mise en conformité ?

Le Net Expert : Denis JACOPINI, vous êtes spécialisé dans l'accompagnement des PME dans la mise en conformité avec le RGPD depuis plusieurs années. Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité avec le RGPD ?

Si le 25 mai 2018 vous n'avez pas terminé votre mise en conformité avec le RGPD ou pire, vous venez à peine de l'initier pour votre entreprise, association ou administration, stricto sensu, en tant que responsable de traitement pénalement responsable, vous devenez amendable et les sanctions encourues, forcément pécuniaires selon les cas, pourraient être accompagnées de peines de prison comme le précise l'article 226-17 du Code pénal.
Ainsi, le Règlement sera « obligatoire dans tous ses éléments et directement applicable dans tout État membre », dont la France dès le 25 mai 2018, et puisqu'il s'agit d'un règlement, celui-ci entrera directement en vigueur, sans nécessiter de législation de transposition.
En réalité, avant que soient engagées des sanctions à votre encontre, vous serez contacté par la CNIL, laquelle vous demandera certainement de justifier les mesures prises à l'égard du Règlement Européen. Il est clair qu'au plus vous faites preuve de négligence, de mauvaise foi et de résistance, les sanctions risquées se rapprocheront du maximum à savoir la plus grande valeur entre 4% de votre chiffre d'affaire mondial ou 20 millions d'euros.
Si par contre, vous avez entamé une démarche de mise en conformité à savoir au minimum commencé à suivre une formation, désigné officiellement une personne (interne ou externe à votre entreprise) à cette démarche réglementaire et même si vous en êtes seulement au stade où vous avez commencé à établir la liste de vos traitements avec les risques inhérents à la vie privée et aux libertés fondamentales des propriétaires des données à caractère personnel et si possible vous avez commencé à mettre en place des mesures correctives, vous montrerez ainsi à l'autorité administrative indépendante de contrôle du bon respect de la réglementation relative à la protection des données à caractère personnel (la CNIL en France) que vous avez pris en compte cette démarche dans votre organisation, pris au sérieux des défaillance en matière juridique ou technique de votre organisation et que des améliorations sont en cours. L'ensemble des démarches accomplies même après le 25 mai 2018 joueront en votre faveur en anéantissant les risques de sanction, bien évidemment à condition que vous ne fassiez aucune victime en cas de fuite de données avant.

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

Réagissez à cet article

Source : Denis JACOPINI (Expert Informatique spécialisé RGPD)

La cybercriminalité, un vrai risque pour les chefs d'entreprises | Denis JACOPINI

La cybercriminalité, un vrai risque pour les chefs d'entreprises

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages.
Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les entreprises.

Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours…) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable.La sécurité informatique est aussi une priorité pour la bonne marche des systèmes industriels (création et fourniture d'électricité, distribution d'eau…). Une attaque informatique sur un système de commande industriel peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.
Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise.
Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses et faciles à mettre en oeuvre dans l'entreprise.

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
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : Denis JACOPINI

Le Crowdfunding, risques, pièges et précautions à prendre | Denis JACOPINI

Le Crowdfunding, désigne le financement participatif.Est-il risqué ?Quels sont ses pièges ?Quelles sont les précautions à prendre ?

Attaque informatique TV5 Monde – Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8 | Denis JACOPINI

	Attaque informatique TV5 Monde -Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8

A la suite de l'attaque informatique ayant visé TV5 Monte, le 9 avril dernier, pendant qu'il se trouvait à un Colloque international sur la Cybercriminalité à Montpellier organisé par Adel JOMNI, Denis JACOPINI a été interviewé par un journaliste de Canal Plus et certains propos retenus pour le JT de 20h45 sur Direct 8.

D'après-vous, pourquoi les pirates ont choisi la chaîne de télévision TV5 Monde comme cible de leur attaque informatique ?Lorsque des pirates ou des cybercriminels décident d'attaquer un système informatique, il le font principalement pour les raisons suivantes :- A la suite d'une sorte de défi qu'ils se sont lancés afin de prouver leur capacité à pirater un système qui s'est par exemple déclaré comme système inviolable…- Afin de récolter de l'argent soit en menaçant de diffuser des informations secrètes, soit en vendant les informations piratées, soit en prenant en otage un serveur en le bloquant et tout cela, contre rançon.

– Ou bien, dans le but de diffuser un message idéologique, prônant un message politique, religieux… Dans ce cas, l'objectif premier des cyber-attaquants est la diffusion à grande échelle d'un message (c.f. les deffaçages de plus de 25000 sites Internet à la suite des attentats contre Charlie Hebdo). Que le plus de personnes possibles puisse prendre connaissance d'un message en y associant une sensation de puissance, tel a été le type d'attaque contre TV5 Monde. Cette attaque, a été destinée avant tout à diffuser un message idéologique, en touchant un média à couverture mondiale pour qu'on parle le plus possible des attaquant et de leur symbole.

Quelle a été la technique utilisée lors de l'attaque des serveurs de TV5 Monde ?

Les cybercriminels utilisent généralement 2 types de méthodes pour pénétrer dans un système informatique :

– la recherche de failles

– la naïveté d'un destinataire à un e-mail

C'est un voire même plusieurs e-mails, de type phishing qui semblent être à l'origine, depuis probablement plusieurs semaines ou mois, de l'intrusion du système informatique de TV5 monde par les cybercriminels. Une fois introduits dans le système informatique, l'accès invisible ou silencieux à des informations confidentielles ou secrètes permet ensuite de trouver les clefs autorisant de se répandre dans un réseau et contaminer ainsi le plus possibles d'organes sensibles ou stratégiques.

Une fois tous ces accès ainsi possibles, il suffit de coordonner une attaque simultanée de tous ces fruits devenus véreux pour donner l'impressionnante vision d'un arbre prêt à tomber.

« Il suffit d'envoyer tous les jours un email avec un virus auprès de différentes personnes de différents services et à un moment ou un autre il va bien y a voir quelqu'un qui va l'ouvrir.

Son vrai travail va commencer lorsque quelqu'un aura mordu à l'hameçon »

Peut-on conclure que n'importe quelle chaines de télévision peuvent être victime de cyber-attaques telles que celle dont a été victime TV5 monde ?

La faille qu'ont exploité les cybercriminels dans le cadre de l'attaque informatique de TV5 monde est une faille humaine. En effet, recevoir un e-mail nous incitant à cliquer sur un lien qui va contre notre volonté et de manière complètement invisible changer dans son ordinateur un logiciel malveillant chargé, de manière tout aussi silencieuse, de prendre le contrôle de notre ordinateur est devenu le moyen d'attaque le plus utilisé.

Les systèmes informatiques des chaines de télévision sont certes équipées de moyens de protection techniques contre les virus, les codes malveillants et autres types d'attaques, mais les cybercriminels auront toujours un coup d'avance en exploitant la faille humaine, principalement par manque de connaissance ou manque de formation de la part des utilisateurs.

Existe t-il un moyen de se protéger contre ce type d'attaque ?

Les organismes et entreprises ont prix trop de retard pour mettre en place des politiques de sécurité informatique. Quand on voit qu'en 2013, moins de 100 000 entreprises en France s'étaient mises en conformité avec la CNIL, excellent point de départ pour mettre en place des mesures de sécurité sur les données personnelles, il y a de quoi s'inquiéter sur la manière dont nos données (mot de passe y compris) sont sécurisées.

Commencer par se mettre en conformité avec la CNIL serait un bon début…

http://www.lenetexpert.fr/wp-content/uploads/2015/04/Denis-JACOPINI-interviewé-par-journaliste-Canal-plus-pour-JT-de-Direct-8.mp4

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://www.bfmtv.com/culture/l-attaque-contre-tv5monde-enclenchee-des-fin-janvier-877334.html

Procédure à suivre pour demander l'aide juridictionnelle | Denis JACOPINI

Comment demander l'aide juridictionnelle

Il vous semble qu'un logiciel espion se cache dans votre iphone, votre smartphone, votre ordinateur, ou votre téléphone ?
Vous soupçonnez être victime d'espionnage informatique ?
Vous souhaitez utiliser les services d'un #expert informatique pour faire analyser votre appareil ?
Avant d'engager les services d'un expert informatique,vérifiez si vous n'avez pas droit à une prise en charge par l'état de vos frais juridiques.

Vous êtes ou il vous semble être victime d'espionnage de votre ordinateur, de votre téléphone ou de votre smartphone ?

Vous souhaitez utiliser les services d'un expert informatique pour faire analyser votre appareil ?

Vous pouvez probablement bénéficier de l'aide

juridictionnelle.

L’aide juridictionnelle, c’est quoi ?

L’aide juridictionnelle vous permet, si vous avez de faibles ressources, de bénéficier d’une prise en charge totale ou partielle par l’État des honoraires et frais de justice (avocat, huissier, expert, etc.).

Si la prise en charge par l’état est totale

Tous vos frais sont pris en charge, à l’exception du droit de plaidoirie fixé à **13 €** dû devant certaines juridictions et à payer à votre avocat.

Attention
Les sommes engagées avant la demande d’aide juridictionnelle ne sont pas remboursées.

Si la prise en charge par l’état est partielle

L’État ne prend en charge qu’une partie des honoraires d’avocat. Vous devez lui verser des honoraires complémentaires à fixer avec lui avant le procès.

Les autres frais relatifs aux instances, procédures ou actes pour lesquels l’aide juridictionnelle partielle vous a été accordée (frais d’expertise, d’enquête sociale, droit d’enregistrement, etc.) sont totalement pris en charge par l’État.

Remarque
L’aide juridictionnelle (totale ou partielle) ne couvre pas les frais auxquels vous pouvez éventuellement être condamné à l’issue du procès (condamnation aux dépens, dommages et

intérêts).

Comment demander l’aide juridictionnelle ?

Formulaire de demande d’aide juridictionnelle – Cerfa n°12467*01

Site Internet sur l’aide juridictionnelle du site Service-Public.fr

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

Références :

Loi n°91-647 du 11 juillet 1991 relative à l’aide juridique

Décret n°91-1266 du 19 décembre 1991 relatif à l’aide juridique

Arrêté du 23 novembre 2011 sur les procédures visées par le décret du 15 février 1995 relatif aux droits de plaidoirie

Comment vérifier si votre site Internet a été victime d'un Hackeur | Denis JACOPINI

	Que ça soit à cause d'une simple erreur de frappe ou du fait que votre site Internet a été Hacké, l'auteur, l'éditeur ou le rédacteur en chef d'un site Internet peut être pénalement responsable des conséquences causées par son contenu non désiré.

Afin de vérifier si votre site Internet a été Hacké, voici quelques conseils pour vérifier si votre site Internet a été victime d'un Hackeur :

Que votre site Internet ait été victime d'un hackeur ou que votre site Internet ait été victime d'un pirate sont deux choses différentes.

Le pirate va pomper une partir ou la totalité du contenu de votre site Internet. Le hackeur va modifier le contenu de votre site Internet dans un but de malveillance.

Les conseils que je vais vous donner concernent le cas où un site Internet a été Hacké.

DU CONTENU ETRANGE APPARAIT ?

En premier lieu, consultez votre site Internet sur plusieurs ordinateurs ayant des systèmes d'exploitation et des navigateurs différents afin de vérifier si un affichage anormal apparaît.

UN ANTIVIRUS DECLENCHE UNE ALERTE A L'OUVERTURE DE VOTRE SITE INTERNET ?

Un message d'alerte de votre antivirus est aussi un bon indicateur de la présence éventuelle d'un code suspicieux sur votre site Internet.

Première solution : Depuis votre dernière sauvegarde vous n'avez plus fait de modifications :

Restaurez les pages Web ou la base de donnée contaminée.

Seconde solution : Vous n'avez pas de Sauvegarde de votre site Internet ou la sauvegarde est trop vieille :

Dans ce cas, vous allez devoir résoudre le problème à la main.

COMMENT TESTER VOTRE SITE INTERNET

Enfin, si vous ne savez pas si votre site Internet a été hacké, vous pouvez le vérifier en utilisant les outils suivants :

https://www.virustotal.com/url

VirusTotal est un service gratuit qui *analyse les fichiers et URL suspects*, et facilite la détection rapide des virus, vers, trojans et tous types de malwares.

http://www.urlvoid.com

URLVoid.com is a free service developed by NoVirusThanks Company Srl that allows users to scan a website address with multiple website reputation engines and domain blacklists to facilitate the detection of possible dangerous websites, used to distribute malware and spyware or related to fraudulent activities.

http://urlquery.net
Query.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis.

http://wepawet.iseclab.org/
Dans ce cas, vous allez devoir résoudre le problème à la main.

COMMENT SE PROTEGER D'UN HACKEUR ?

Voici quelques astuces simples vous aideront a protéger votre site efficacement contre les pirates et hackers de l'internet :

Ces techniques sont efficace contre les hackers débutants.

- Avoir un hébergeur de qualité et lui même utilisant des surveillances automatiques et permanentes.
- Mettez à jour systématiquement le système d'exploitation de votre serveur ainsi que toutes les applications liées à l'hébergement des sites internet, du FTP, des messageries et des bases de données.
- Supprimer l'utilisateur « admin » des logiciels et créez le votre
- Mot de passe sécurisé (minuscules, majuscules, chiffres et symboles)

Cet article vous à plu ? Laissez-nous un commentaire

(notre source d’encouragements et de progrès)

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

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

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

---

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

Sources : Denis JACOPINI

https://www.cnil.fr/fr/comment-se-passe-un-controle-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					
	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 lus 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.

Réagissez à cet article

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 solution 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/delib/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 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)