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

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

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

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

1- DÉSIGNER UN PILOTE

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

2- CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

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

3- PRIORISER LES ACTIONS À MENER

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

4- GÉRER LES RISQUES

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

5- ORGANISER LES PROCESSUS INTERNES

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

6- DOCUMENTER LA CONFORMITÉ

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

Pour **cartographier vos traitements** de données personnelles, vous devrez avoir une méthode, des outils, collecter des informations à la fois techniques et organisationnelles.
Pour **prioriser les actions** à mener vous devrez identifier précisément les traitements à risques, les données sensibles et connaître les solutions techniques applicables.
Pour **gérer les risques**, vous devrez appliquer une méthode relative à cette obligation. Proche de la méthode EBIOS, l'analyse d'impact relative à la protection des données (DPIA) est le passage obligatoire pour tout organisme (entreprise ou association) disposant de salariés ou détenant des données sensibles appartenant à des tiers.
L'**organisation des processus internes** nécessite une excellente connaissance des menaces et des risques. Une certification relative à une norme ISO 27001 ou 27005 nous paraît essentielle.

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

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

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

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

CONTENU DE NOTRE FORMATION RGPD :
Parce que les piratages sont de plus en plus fréquents et dangereux, à tout moment, nos données personnelles médicales, bancaires et confidentielles peuvent se retrouver dans la nature à cause d'un professionnel négligeant ayant manqué à son obligation de sécurité des données vis-à-vis de ses clients, salariés, fournisseurs…
Pour ne pas que vous deveniez ce professionnel négligeant risquant d'être sanctionné pénalement et par une mauvaise réputation, un règlement Européen (le RGPD) entrant en application le 25 mai 2018, clarifie les obligations que tous les professionnels devraient déjà respecter.
Venez découvrir lors de cette journée de formation les points importants de ce règlement Européen et la méthode à suivre pour continuer sereinement votre activité.

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

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

---

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

- 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

Réagissez à cet article

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

RGPD : Ca ne se passera plus comme ça !

RGPD : Ca ne se passera plus comme ça !

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

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

Complément de Denis JACOPINI :

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

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

• Vous avez mis en œuvre un traitement de données personnelles ;

• Ces données ont fait l'objet d'une violation (destruction, perte, altération, divulgation ou un accès non autorisé à des données personnelles, de manière accidentelle ou illicite) ;

• Cette violation est intervenue dans le cadre de votre activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de votre service de téléphonie ou d'accès à d'internet).

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

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

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

Le formulaire à utiliser est celui-ci :

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

---

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

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

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

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

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

RGPD : Vol de données : la nouvelle norme

RGPD : Vol de données : la nouvelle norme

A six mois de l'entrée en vigueur du nouveau règlement européen sur la protection des données personnelles (RGPD) le 25 mai 2018 prochain, Proofpoint, spécialiste de la cybersécurité, dévoile les résultats de son étude paneuropéenne (Royaume-Uni, France, Allemagne) analysant le niveau de préparation des entreprises.

Les cyberattaques sont malheureusement devenues monnaie courante pour les entreprises qui doivent désormais intégrer pleinement les risques associés à leurs stratégies de sécurité pour se protéger. A l'image du piratage d'Equifax exposant les données personnelles de plus de 145 millions de citoyens américains ou du ransomware Wannacry ayant affecté plus de 200,000 ordinateurs dans 150 pays, tout le monde est concerné.

La France, semble particulièrement affectée, avec 61% des entreprises françaises qui déclarent avoir subi un vol de données personnelles durant les deux années écoulées (54% au Royaume Uni et 56% en Allemagne) et 78% d'entre elles qui redoutent un vol de données dans les 12 mois à venir (54% au Royaume-Uni et 46% en Allemagne).

Niveau de préparation RGPD : un décalage évident entre perception et réalité

Si les décideurs IT français semblent mieux préparés que leurs voisins (51% des répondants français pensent que leur organisation est déjà en conformité avec la réglementation RGPD, contre 45% au Royaume-Uni et 35% en Allemagne), l'étude révèle que plus d'une entreprise française sur cinq (22%) ne sera toujours pas en conformité avec la réglementation lors de son entrée en vigueur en mai 2018 (23% au Royaume-Uni et 34% en Allemagne). Un résultat finalement peu surprenant, considérant que seules 5% des entreprises auraient effectivement mis en place toutes les stratégies de gestion de données nécessaires pour garantir cette mise en conformité.

Les décideurs IT semblent pourtant conscients des enjeux, puisque 66% des répondants confient que leur budget a augmenté en prévision de l'entrée en vigueur de RGPD. Plus de sept entreprises sur dix en Europe ont par ailleurs monté des équipes projet dédiées RGPD et plus d'une sur quatre a désigné un responsable de la protection des données. A l'épreuve des faits, et alors que les entreprises avaient deux ans pour se préparer (adoption de la réglementation en avril 2016), seuls 40% des répondants révèlent que leur organisation a rempli un formulaire de mise en conformité RGPD…[lire la suite]

Source : *RGPD : 1 entreprise française sur 5 ne sera pas en conformité ! | UnderNews*

Jouets connectés : Dangers pour votre vie privée dit la CNIL

Jouets connectés : Dangers pour votre vie privée dit la CNIL

La Présidente de la CNIL met en demeure la société GENESIS INDUSTRIES LIMITED de procéder à la sécurisation de jouets connectés à destination d'enfants : la poupée « My Friend Cayla » et le robot « I-QUE ».

Le robot « I-QUE » et la poupée « My Friend Cayla » sont des jouets dits « connectés ». Ils répondent aux questions posées par les enfants sur divers sujets tels que des calculs mathématiques ou encore la météo. Les jouets sont équipés d'un microphone et d'un haut-parleur et sont associés à une application mobile téléchargeable sur téléphone mobile ou sur tablette. La réponse est extraite d'Internet par l'application et donnée à l'enfant par l'intermédiaire des jouets.

Alertée, en décembre 2016, par une association de consommateurs sur le défaut de sécurité des deux jouets, la Présidente de la CNIL a décidé de réaliser des contrôles en ligne en janvier et novembre 2017. Elle a par ailleurs adressé un questionnaire en mars 2017 à la société située à Hong-Kong.

Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom…) mais également des informations renseignées dans un formulaire de l'application « My Friend Cayla App ».

Plusieurs manquements à loi Informatique et Libertés ont été constatés dont notamment :

1.

Le non-respect de la vie privée des personnes en raison d'un défaut de sécurité

Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou « appairer ») un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier (par exemple, avec un code PIN ou un bouton sur le jouet).

La personne située à une telle distance est en mesure d'entendre et d'enregistrer les paroles échangées entre l'enfant et le jouet ou encore toute conversation se déroulant à proximité de celui-ci.

La délégation de la CNIL a également relevé qu'il était possible de communiquer avec l'enfant situé à proximité de l'objet par deux techniques :

- soit en diffusant via l'enceinte du jouet des sons ou des propos précédemment enregistrés grâce à la fonction dictaphone de certains téléphones ;
- soit en utilisant les jouets en tant que « kit main libre ». Il suffit alors d'appeler le téléphone connecté au jouet avec un autre téléphone pour parler avec l'enfant à proximité du jouet.

La Présidente a considéré que l'absence de sécurisation des jouets, permettant à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter, à l'insu des enfants et des propriétaires des jouets et d'avoir accès aux discussions échangées dans un cercle familial ou amical, méconnait l'article 1er de la loi Informatique et Libertés selon lequel l'informatique « *ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

2.

Le défaut d'information des utilisateurs des jouets

Alors que des informations personnelles sont traitées par la société, les contrôleurs de la CNIL ont constaté que les utilisateurs des jouets ne sont pas informés des traitements de données mis en œuvre par la société…[lire la suite]

Source : *Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité | CNIL*

Ce qu'il faut savoir sur les jouets connectés

Ce qu'il faut savoir sur les jouets connectés

S’ils s’invitent en nombre dans les magasins et sur les listes au Père Noël, les jouets connectés suscitent quelques craintes. Voici un petit guide pour s’y retrouver.

Tablettes, robots, peluches, jeux de société… Difficile de ne pas trouver une catégorie de jouets dont un ou plusieurs modèles n’aient pas une version connectée. De récents scandales montrent que le secteur n’est pas encore tout à fait au point pour que les plus jeunes puissent s’amuser en toute sécurité. En sept questions, Pixels fait le tour de cette tendance et des précautions à prendre pour que Noël ne tourne pas à une mise sur écoute.

[…]

Si l’on considère les jouets connectés au regard de la loi informatique et libertés, plusieurs questions s’avèrent importantes :

• le fabricant informe-t-il de façon claire les utilisateurs (en tout cas les parents) sur le fait que le jouet enregistre des données ? Recueille-t-il clairement leur consentement ? Le jouet ou l’appli invitent-ils bien les parents à réaliser cette étape importante au lieu de laisser l’enfant passer rapidement dessus ?

• est-il pertinent et nécessaire pour le fabricant de récupérer ces données ? Par exemple, est-il utile de demander l’adresse postale ou le nom complet d’un enfant pour faire fonctionner un jouet ? A quoi peuvent servir ces données au fabricant ?

• s’agissant de la sécurité de ces données : un mot de passe fort est-il requis ? Comment les données sont-elles chiffrées, où sont-elles stockées, et pendant combien de temps ? Qui peut y accéder ?

Les fabricants font-ils attention ?

Difficile de répondre puisque les fabricants ne sont mis en défaut que lorsqu’un problème de protection des données ou de vulnérabilité du jouet surgit, souvent bien après la commercialisation du produit.

En ce qui concerne la France, certains fabricants consultent en amont la Commission nationale informatique et libertés (CNIL) pour s’assurer d’être en conformité avec la loi. D’autres sont moins scrupuleux par souci d’économies. Ils utilisent par exemple des composants standards, parfois peu sécurisés, pour que le jouet ne soit pas trop cher.

Il y a aussi une limite technique. Si, après la mise sur le marché, un fabricant souhaite apporter une correction, il peut le faire sur une application ou un logiciel mais pas sur le jouet lui-même. Il faudrait rappeler le produit…[lire la suite]

Source : *Ce qu’il faut savoir sur les jouets connectés*

Vol de données chez Uber :

L’état Français demande des explications

	Vol de données chez Uber : L’état Français demande des explications

Le secrétaire d'État au Numérique a écrit jeudi au PDG d'Uber, Dara Khosrowshahi, après l'annonce du piratage des données personnelles de 57 millions d'usagers.

Le secrétaire d'État au Numérique Mounir Mahjoubi a écrit jeudi au PDG d'Uber, Dara Khosrowshahi, après l'annonce du piratage des données personnelles de 57 millions d'usagers, pour lui demander des explications sur d'éventuelles victimes françaises.

« Face au danger que représente l'exploitation de ces données, je souhaite vous exprimer mon inquiétude quant à l'éventuelle présence en très grand nombre de clients et chauffeurs français » parmi les victimes, souligne Mounir Mahjoubi, dans un courrier. « Pouvez-vous à ce jour nous indiquer si des utilisateurs français sont concernés et si oui combien, et de quel type sont les données qui ont été dérobées », interroge-t-il. Le secrétaire d'État demande aussi « quelles mesures techniques et organisationnelles sont mises en place pour informer et accompagner les utilisateurs ».

Noms, adresses électroniques et numéros de téléphone.

Uber n'a pas détaillé qui sont les victimes de cette fuite d'informations remontant à la fin 2016, et qu'il avait dissimulée, mais de nombreux Français sont vraisemblablement concernés. Le chiffre de 57 millions est en effet énorme, quand l'ancien patron Travis Kalanick déclarait en octobre 2016 -plus ou moins au moment des faits- compter 40 millions d'utilisateurs actifs dans le monde. Selon Uber, les noms, adresses électroniques et numéros de téléphone des victimes ont été subtilisés. Le groupe américain de réservation de voitures avec chauffeur affirme qu'aucune information bancaire n'a été exfiltrée, pas plus que les dates de naissance et les historiques de trajets.

Le secrétaire d'État s'étonne qu'Uber n'ait « pas signalé cet incident ». Mounir Mahjoubi s'étonne également de ce qu'Uber n'ait « pas signalé cet incident » auprès de la Commission nationale de l'informatique et des libertés (Cnil) et de l'Agence nationale de la sécurité des systèmes d'information (Anssi), responsables respectivement de la protection des citoyens et de la coordination de la défense française contre les pirates informatiques, qui ont été mises en copie de son courrier. Il aurait également apprécié que le groupe américain se signale « auprès des utilisateurs concernés ».

Mahjoubi souhaite que l'entreprise informe les utilisateurs concernés et les autorités. « Au regard du nombre de vos clients, vous avez une importance qui vous donne des responsabilités », souligne Mounir Mahjoubi, rappelant qu'un règlement européen rendra en mai prochain les entreprises responsables des données personnelles qu'elles détiennent, et leur imposera de signaler rapidement les incidents. « Au regard du danger existant, nous aimerions que vous informiez volontairement les utilisateurs concernés ainsi que les autorités françaises », insiste le secrétaire d'État au Numérique…[lire la suite]

Réagissez à cet article

Source : *Piratage d’Uber : Mahjoubi demande des explications*

RGPD : les petites entreprises tout aussi concernées que les grandes

RGPD : les petites entreprises tout aussi concernées que les grandes

---

Le règlement général européen sur la protection des données sera mis en œuvre le 25 mai 2018 pour améliorer la protection et la confidentialité des données et responsabiliser davantage les entreprises en développant l'auto-contrôle. Celles-ci devront dorénavant s'assurer que toutes les données qu'elles stockent sont en conformité avec la réglementation.

Le 25 mai prochain, toutes les entreprises devront se conformer à la nouvelle réglementation générale des données personnelles (RGPD). Celle-ci vise à établir des règles claires et unifiées pour que les individus puissent mieux contrôler les données qui les concernent. Les obligations visent toutes les entreprises, en B to B comme en B to C, quelle que soit leur taille, à partir du moment où elles collectent, traitent, gèrent et utilisent des données, que ce soit des fichiers collaborateurs en interne ou des données sur leurs clients ou fournisseurs. « Un ancien candidat qui a envoyé son CV à l'entreprise pour y postuler constitue par exemple une donnée collectée » cite Nathalie Rouvet Lazare, PDG de Coheris qui édite des solutions CRM et analytiques sur le sujet.

Toutes les données stockées sont concernées

Les données considérées comme personnelles sont nombreuses : nom, adresse, localisation, identifiant, date de naissance, IP…, autrement dit toutes les données qui permettent d'identifier une personne. Même si les données ne sont pas utilisées et traitées, à partir du moment où elles sont stockées au sein de l'entreprise, elles sont concernées par la réglementation. Même chose en termes de forme : tous les fichiers, du tableur Excel aux bases de données de prospects, salariés ou visiteurs d'un site Internet ou d'une boutique physique, sont visés. Nathalie Rouvet Lazare se veut rassurante : « Les petites entreprises doivent elles aussi se mettre en ordre de marche et établir une feuille de route. Il ne faut pas y voir une usine à gaz ou une contrainte de plus mais utiliser cette nouvelle réglementation comme une opportunité pour optimiser les données de l'entreprise ». Si celles-ci ont tendance à collecter un maximum de données, au final, peu d'entre elles les utilisent. « Elles devront dorénavant mener une réflexion préalable sur leur objectif pour chaque donnée collectée. »

Se conformer au règlement en 3 étapes

Pour mettre en place une gouvernance des données personnelles, les entreprises doivent commencer par :

• nommer une personne référente au sein de l'entreprise qui sera le pilote responsable de la mise en place des process et des outils. « Si les entreprises n'ont pas l'obligation légale de nommer un DPO (Data Protection Officer ou Délégué à la Protection des Données), il est essentiel de désigner un porteur de projet sur le sujet. »

• réaliser un audit, soit cartographier toutes les données personnelles et sensibles de l'entreprise, définir dans quels types de fichiers elles sont utilisées et comment elles sont gérées.

• passer au crible ses obligations et définir ses process et responsabilités pour s'assurer qu'elle est en conformité avec la loi.

L'occasion de mettre en place plusieurs bonnes pratiques pour répondre aux nouvelles obligations liées à la RGPD, comme un process pour protéger les données dès leur conception – data protection de by design–, la vérification de la protection effective de ses données, l'élimination des données récoltées de façon illicite ou déloyale, la révision de ses procédures de consentement qui doit être clair et circonstancié. Et si l'entreprise souhaite partager ses données personnelles avec ses partenaires, elle doit en préciser l'identité et la finalité du partage. C'est ce que l'on appelle la récolte opt-in. Enfin, avec la RGPD, les entreprises doivent être en mesure de respecter l'exercice du droit d'opposition, de rectification, d'accès direct, de portabilité et d'effacement des données…[lire la suite]

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

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

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

---

Réagissez à cet article

Source : *Protection des données : les petites entreprises tout aussi concernées que les grandes*

RGPD : Ce que les consommateurs doivent savoir

	**RGPD : Ce que les consommateurs doivent savoir**

Les consommateurs doivent comprendre clairement ce qu'ils acceptent comme traitements sur les sites e-commerce et la portée de leurs consentements.

Les techniques modernes de marketing e-Commerce (retargetting, suggestions de produits…) doivent être explicitement acceptées par les particuliers. Ils disposent également d'un accès direct à leurs informations personnelles. En pratique, ils pourront demander la portabilité de leurs informations (données de commandes, listes d'envie…) et obtenir un double consentement pour leurs enfants. En cas de fuite de données, l'internaute sera informé dans les 72 heures par l'entreprise, la responsabilité pouvant incomber au sous-traitant responsable de la fuite ou à l'hébergeur si ce dernier a été attaqué. Pour s'assurer du respect de ces nouveaux droits, le législateur a rendu possibles les actions collectives via des associations…[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
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 : 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

Réagissez à cet article

Source : *Le RGPD : 81% des entreprises ne seront pas en conformité en mai 2018 – Global Security Mag Online*

RGPD : Comment le mettre en oeuvre dans le e-Commerce

RGPD : Comment le mettre en oeuvre dans le e-Commerce

D'ici mai 2018 toutes les entreprises devront respecter la nouvelle réglementation. Cette mise en œuvre implique une bonne compréhension à la fois des obligations et des moyens d'y parvenir.

Les sites e-Commerce devront assurer le plus haut niveau possible de protection des données. Pour garantir la sécurité des données personnelles de leurs clients les marchands devront déployer tous les moyens techniques et respecter des règles strictes : la mise en œuvre d'un registre de consentements, la conservation des données, la sécurisation des mails transactionnels, le cryptage des mots de passe…. Un délégué à la protection des données (DPO) sera désigné pour assurer la mise en place et le suivi de ces actions.

On passe dans une logique de responsabilisation totale de l'entreprise, une nécessité au regard des plus de 170 000 sites ne seront pas en conformité avec le règlement européen en mai 2018.

Rappelons que chaque jour des milliers d'attaques visent la totalité des acteurs du e-Commerce. La sécurité des données et des infrastructures techniques sont les enjeux majeurs du monde du web. Le nombre total de cyber-attaques a augmenté de 35% en l'espace d'un an. En France nous en avons recensé plus de 15 millions au 1er trimestre 2017 ce qui représente 4,4% des attaques mondiales. Un cadre contraignant pour les entreprises et des impacts majeurs à court terme Le baromètre RGPD1 démontre qu'à ce jour 44% des entreprises considèrent déjà qu'elles ne seront que partiellement conformes. Les sanctions en cas de manquement aux obligations imposées par la règlementation sont financières et indexées sur le chiffre d'affaires de l'entreprise. Elles peuvent atteindre de 10 à 20 millions d'euros ou 2 à 4% du CA, la sanction la plus élevée sera retenue. Un nouveau concept émerge : le « Privacy By design », un gage de qualité et de réassurance pour les entrepreneurs à la recherche d'une sécurisation optimale des données clients. Un site conçu en « Privacy by Design » garantit qu'aucun module n'a été ajouté à la structure du site et que la solution a été élaborée avec la protection des données comme prérequis à chaque étape de la mise en ligne du site…[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
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 : 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

Réagissez à cet article

Source : *Le RGPD : 81% des entreprises ne seront pas en conformité en mai 2018 – Global Security Mag Online*

RGPD : Quel est le profil idéal pour devenir DPO

RGPD : Quel est le profil idéal pour devenir DPO

Aujourd'hui, 47 % des CIL sont issus de l'IT et 19 % possèdent un profil plutôt juridique, selon les chiffres de la Cnil.

Le reste est un panachage assez large, allant du documentaliste au responsable administratif. A priori, le poste de DPO devrait correspondre à ces mêmes profils. « *Il y a cependant aujourd'hui une tendance à penser que le DPO devra surtout disposer d'un profil juridique. Mais c'est une erreur. Il faut préserver la richesse de profils qui a fait la force des CIL, et laisser notamment le poste de DPO ouvert à des informaticiens* », souligne Bruno Rasle (Président de l'AFCDP). Ayant un rôle éminemment transversal, le DPO doit être un « *très bon communicant* », indique-t-on à la Cnil. Outre la technique et le juridique, il doit également bien connaître les enjeux business, afin de ne pas se positionner comme un frein au développement de l'entreprise, mais davantage comme un garant du respect de la « privacy ». Un respect qui peut d'ailleurs être très positif en termes d'image de marque, indique l'AFCDP. Au final, il s'agit donc d'un poste très « politique », plutôt accessible aux collaborateurs expérimentés…[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
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 : 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

Réagissez à cet article

Source : *Data Protection Officer : un gardien pour les données personnelles*