RGPD : Ce qui va changer pour les professionnels de santé

	**RGPD : Ce qui va changer pour les professionnels de santé**

Fin des déclarations Cnil, demandes de consentement et sanctions renforcées, une nouvelle réglementation européenne* va venir chambouler la gestion des données personnelles en magasin. En tant que commerçants et professionnels de santé, vous collectez et transmettez des données relatives à vos clients. Le GDPR (General Data Protection Régulation) devra donc s'appliquer à votre point de vente. Zoom sur ce qui change dès le 25 mai 2018.

Registre des traitements et désignation d'un délégué à la protection des données

Quotidiennement vous gérez, stockez et envoyez les données de santé de vos clients que ce soit pour la pratique du tiers payant ou effectuer une commande auprès de vos fournisseurs. Identité, numéro de Sécurité sociale, facturation, prescription… vous êtes amenés à traiter des données personnelles, qui doivent actuellement faire l'objet d'une déclaration auprès de la Cnil (Commission nationale de l'informatique et des libertés). Mais bientôt, vous n'aurez plus besoin de cette formalité préalable.

En effet, le règlement européen sur la protection des données personnelles repose sur une logique de conformité, dont les acteurs seront désormais responsables. En d'autres termes, le poids de la procédure administrative va être transféré de la Cnil. **Dès le 25 mai 2018, vous devrez être en possession et tenir un « registre des traitements mis en œuvre ».** Ce dernier devra notamment spécifier :

- les catégories de données traitées ;
- la finalité ;
- les différents destinataires ;
- la durée de conservation.

« Ce registre informatisé permettra au professionnel de se ménager des preuves vis-à-vis de la Cnil. Il prouve son adhésion à un code de conduite, explique Maître Cécile Vernudachi, avocate au Barreau de Paris. Les grandes enseignes pourront également désigner un délégué à la protection des données, qui deviendra le point de contact avec la Cnil et un véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Dans les plus petites structures, ce ne sera pas une obligation », précise-t-elle.

Consentement renforcé et transparence

Le règlement européen impose également la mise à disposition d'une information claire, intelligible et aisément accessible à vos clients. Il définit en ce sens l'expression du consentement : « **les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer.** La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe », précise le document.

En d'autres termes, avant chaque devis ou chaque vente, vous êtes tenus d'obtenir le consentement de votre porteur pour pouvoir traiter et transmettre ses données personnelles. « Concernant la correction, seul le patient peut donner son accord pour la transmission de cette donnée, souligne Maître Vernudachi. **Son consentement doit obligatoirement être écrit.** Dans le cadre de l'exécution d'un contrat, il n'y a alors plus de restriction. Toutefois, il est interdit d'utiliser cette information pour la vendre à un tiers ou à des fins marketings et commerciales ».

Spécificité pour les moins de 16 ans :

Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Des sanctions encadrées et graduées

Les responsables de traitement, autrement dit les dirigeants ou chef d'entreprise, les plateformes de services et les complémentaires santé, peuvent enfin faire l'objet de **sanctions administratives importantes en cas de non-conformité au nouveau règlement**. Les autorités de protection peuvent notamment :

- prononcer un avertissement ;
- mettre en demeure l'entreprise ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des amendes dans le cas d'une entreprise, elles peuvent s'élever de 2% à 4% du chiffre d'affaires annuel mondial, en fonction de la catégorie de l'infraction.

Notons que selon l'étude « Crossing the Line » du cabinet KPMG**, les Français sont 2ème sur le podium des consommateurs les plus vigilants quant au traitement de leurs données personnelles. Aussi, le règlement européen sera en vigueur dès le 25 mai 2018. Il vous faut donc être vigilant et vous y préparer dès maintenant !

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

****étude publiée en novembre 2016***

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation 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 : *Ce qui va changer dans les magasins pour le traitement des données personnelles | Acuité*

Nouvelles tensions autour du Privacy Shield entre l'Europe et les USA

Nouvelles tensions autour du Privacy Shield entre l'Europe et les USA

Une coalition d'associations demande à la Commission européenne de suspendre le nouvel accord sur les données personnelles, intitulé Privacy Shield, si les États-Unis ne réforment pas leur politique en matière de renseignement.

Le rejet envers le Privacy Shield ne faiblit pas. Dans une lettre ouverte datée de mars, une coalition d'associations européennes et internationales, dont La Quadrature du Net, demandent aux États-Unis et à l'Union européenne de suspendre l'exécution de ce mécanisme juridique. L'accord transatlantique « *ne donne pas assez de garanties à la protection des données personnelles des Européens* » jugent-elles.
Le **Privacy Shield** est l'accord qui encadre les transferts des données personnelles vers les États-Unis. Il remplace l'ancien Safe Harbor que la Cour de justice de l'Union européenne a invalidé fin 2015 parce que les protections apportées par le droit européen n'étaient pas assurées aux USA.
La raison ? Les lois américaines sur le renseignement actuellement en vigueur outre-Atlantique. « *Au moment de l'adoption de cet accord, plusieurs groupes ont souligné que la loi américaine était inadaptée pour protéger les données des européens et ne satisfaisait pas le critère d'« équivalence substantielle » imposé par la Cour de justice de l'Union européenne* », écrivent les signataires.
Ils rappellent qu'ils « *ont à plusieurs reprises pointé du doigt les défauts présents dans les mécanismes américains de recours et de supervision des violations de la vie privée, les insuffisances dans les limitations de la collecte, l'accès et l'utilisation des données personnelles, et les incertitudes des garanties écrites* ». Pour toutes ces raisons, et sans action du côté américain, la suspension est l'unique solution.
« *Sans réelle réforme de la surveillance, nous pensons qu'il est de votre responsabilité, à défaut d'une meilleure option, de suspendre le Privacy Shield. Nous vous exhortons à clarifier ce positionnement pour vos homologues américains* » ajoutent les associations. Sinon, « *nous considèrerons cela comme un message fort envoyé à l'Union européenne déclarant que nos droits sont sans importance* ».

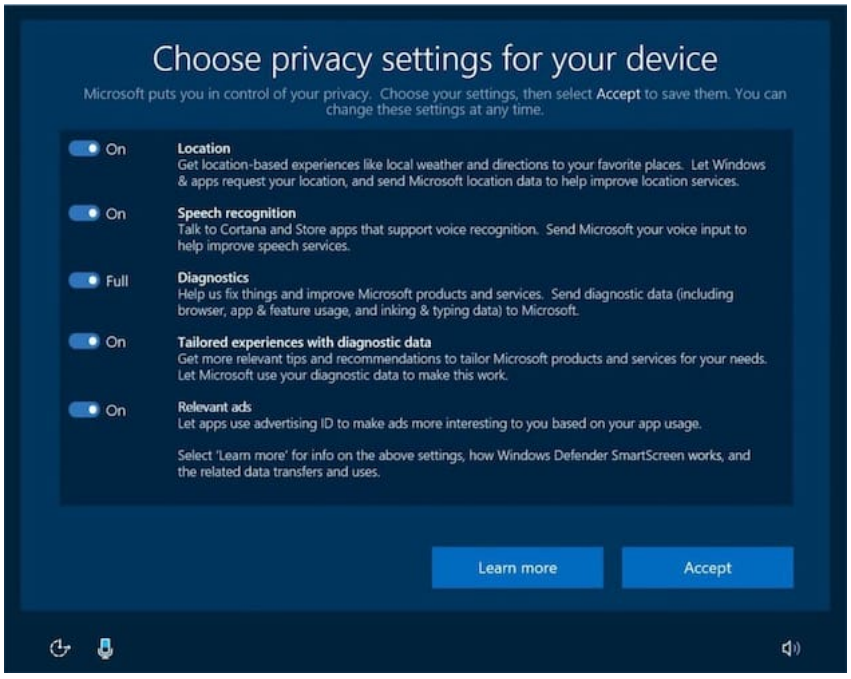
INQUIÉTUDE EN EUROPE

Les associations civiles ne sont pas les seules à s'alarmer des faiblesses du Privacy Shield. L'été dernier, le groupe de l'article 29 (G29), qui rassemble au niveau européen toutes les autorités de protection des données et de la vie privée, comme la Commission nationale de l'informatique et des libertés en France, a ainsi fait part de son inquiétude, après avoir critiqué le Privacy Shield dans un avis du 13 avril 2016…[lire la suite]

Réagissez à cet article

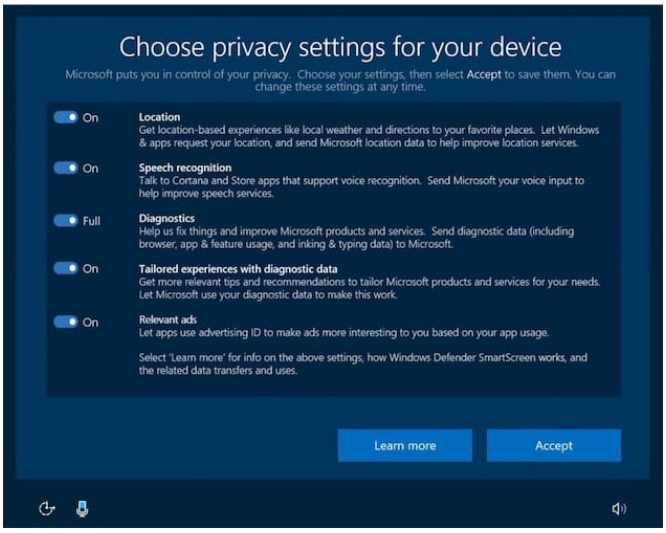
Source : *Privacy Shield : levée de boucliers contre l'accord sur les données personnelles entre l'Europe et les USA – Politique – Numerama*

Les CNIL européennes toujours insatisfaites de la politique de confidentialité de Windows 10



Les CNIL européennes toujours insatisfaites de la politique de confidentialité de Windows 10

En dépit des mesures annoncées par Microsoft, le groupement des autorités européennes de protection des données s'inquiète toujours de la politique de confidentialité de Windows 10, jugée trop évasive.
Reuters rapporte que le G29 a adressé un nouveau courrier à l'éditeur pour lui indiquer que les changements proposés n'étaient pas suffisants. Microsoft envisage de présenter cinq nouvelles options durant le processus d'installation pour limiter ou couper la collecte de données de localisation, reconnaissance vocale, diagnostics, recommandations et publicités ciblées.



Les nouveaux réglages de confidentialité proposés par Microsoft. Cliquer pour agrandir
« *Microsoft devrait clairement expliquer quels types de données personnelles sont exploitées et à quelles fins. Sans cette information, l'utilisateur ne peut pas être renseigné et, par conséquent, son consentement n'est pas valide* », insistent les CNIL européennes…[lire la suite]

A Lire aussi :
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 dessins
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 : *Les CNIL européennes toujours insatisfaites de la politique de confidentialité de Windows 10*

La commission de contrôle des élections veillera au ‘risque d’attaque informatique’

Saisir les autorités en cas de cyberattaque, veiller au respect du principe d'égalité entre les candidats à l'élection présidentielle… La Commission nationale de contrôle de la campagne a été installée ce soir au Conseil d'Etat par le ministre de la Justice.

La commission portera « une vigilance particulière au risque d'attaque informatique de la campagne », a déclaré le garde des Sceaux Jean-Jacques Urvoas. En décembre, l'Agence nationale de la sécurité des systèmes d'information (Anssi) et le Secrétariat général de la défense et de la sécurité nationale (SGDSN) avaient souligné « le risque de cyberattaque à motif politique », a rappelé Jean-Jacques Urvoas.

» Lire aussi : L'Élysée inquiet d'une cyber-menace étrangère pesant sur la présidentielle

« Si un candidat estime qu'il fait l'objet d'une attaque susceptible d'affecter le déroulement de sa campagne, il pourrait saisir la commission », a confirmé son président Jean-Marc Sauvé, à la tête du Conseil d'Etat. Mais il revient d'abord aux candidats et à leurs partis politiques de « mettre en oeuvre les solutions adéquates » pour y faire face, a-t-il toutefois précisé. Si une attaque devait être avérée, la commission – en lien avec le Conseil constitutionnel – demanderait des investigations…[lire la suite]

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

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

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

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

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des 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

Source : *La commission de contrôle des élections veillera au ‘risque d’attaque informatique’*

Les collectivités territoriales cibles des Pirates Informatiques

Les collectivités territoriales cibles des Pirates Informatiques

---

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

FOCUS

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

À LIRE AUSSI
• Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

À LIRE AUSSI
Notre dossier : Données personnelles, un gisement sous haute protection

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

A Lire aussi :
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 dessins
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

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*

Les CNIL européennes s'inquiètent du décret Trump pour le Privacy Shield

Les CNIL européennes s'inquiètent du décret Trump pour le Privacy Shield

---

Les CNIL européennes s'inquiètent du récent décret sur l'immigration du Président Trump. Elles veulent s'assurer que le Privacy Shield n'en souffrira pas.

Alors que Donald Trump a annoncé la présentation d'un nouveau décret sur l'immigration la semaine prochaine, les CNIL européennes se sont penchées sur le premier décret, suspendu par la justice. Celui-ci a été pris le 25 janvier dernier et comportait une clause pouvant avoir un impact sur le récent accord de transfert transatlantique des données : le Privacy Shield.

En effet, la clause numéro 14 du décret indique que « *les agences devront, dans la mesure permise par la loi en vigueur, s'assurer que leurs politiques de protection des données personnelles excluent les non-citoyens américains et les non-résidents permanents autorisés, des protections offertes par le Privacy Act au regard des informations personnelles identifiables* ». Les agences citées dans le texte sont bien évidemment celles du renseignement comme la NSA ou le FBI. Pour autant cette notion de « *pas de protection de la confidentialité pour les citoyens non-américains* » heurte l'essence même du Privacy Shield. Pour mémoire, ce dernier érige comme credo le fait que les données des citoyens européens exportées aux Etats-Unis bénéficient de la même protection que le droit européen…[lire la suite]

A Lire aussi :
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 dessins
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

Source : *Privacy Shield : Les CNIL européennes s'inquiètent du décret Trump | Silicon*

Vous offrez aux hackers des données invisibles sans le savoir

Vous offrez aux hackers des données invisibles sans le savoir

Empreintes digitales, données GPS des photos, réponses aux questions prétendues «secrètes»…: des données sensibles se cachent sur ce que vous publiez sur les réseaux sociaux, même si l'essentiel du risque se concentre sur des informations livrées plus directement encore…

Le « V » de la victoire pourrait être celui des hackers. Un chercheur japonais avertissait début janvier contre le danger contenu dans ce signe parfois associé aux selfies: en montrant vos doigts, vous courez le risque de vous faire voler vos empreintes digitales, prévient Isao Echizu.
Alors que les «données sont le pétrole du 21ème siècle », comme on l'entend à l'envi, nous avons une fâcheuse tendance à livrer les nôtres, intentionnellement, sur les réseaux sociaux, en négligeant bien souvent les règles de confidentialité ou l'utilisation commerciale qui est leur est destinée. Mais la vigilance se complique quand on n'a même pas conscience qu'une donnée en est une…

Attention aux données invisibles…

Permettez-moi d'emprunter vos empreintes

Avec la haute résolution des photos prises par les smartphones, une opération – assez complexe, toutefois, et loin d'être à la portée de tout le monde – peut permettre de récupérer les empreintes. « Or à l'inverse des mots de passe, les empreintes, une fois volées, ne pourront jamais être changées», rappelle à *20 Minutes* Gérôme Billois, expert cybersécurité au cabinet Wavestone.
Il note que si l'avertissement du professeur japonais a fait le tour du monde, « on connaissait le risque depuis 2014 »: un hacker avait montré lors d'une conférence qu'il était parvenu à cloner les empreintes digitales de la ministre allemande de la Défense. Depuis, les empreintes digitales sont de plus en plus utilisées, pour déverrouiller smartphones, objets connectés ou pour réaliser certains paiements.

Des photos très bavardes

Autre donnée invisible, la géolocalisation associée aux photos, la grande majorité étant prise aujourd'hui par des smartphones équipés d'une puce GPS (qui ne sert pas qu'à vous guider sur la route jusqu'à Palavas-Les-Flots). Aux images numériques sont associées tout un ensemble de métadonnées, qui «peuvent renseigner la date, l'heure, voire les données GPS de l'image, la marque, le numéro de série de l'appareil ainsi qu'une image en taille réduite de l'image originale», comme le précise We Fight Censorship, qui indique la marche à suivre pour nettoyer ces métadonnées.«Internet abonde de ces images floutées dont le fichier EXIF contient toujours le document avant floutage», lit-on encore.
En septembre dernier, deux étudiants de Harvard ont pu démasquer 229 dealers grâce aux coordonnées géographiques contenues dans les métadonnées associées à des photos qu'ils avaient prises et postées en ligne.

En huit tweets, tout est dit

Sur Twitter, si la géolocalisation des tweets est désactivée par défaut, beaucoup l'activent. En mai dernier, des experts du MIT et d'Oxford démontraient que huit tweets (d'utilisateurs pour lesquels la géolocalisation est activée) suffisaient à localiser quelqu'un de façon très précise. « Il est extrêmement simple pour des personnes avec très peu de connaissance technique de trouver où vous travaillez ou vivez », expliquaient-ils, à l'issue d'une expérience concluante.

Le secret imaginaire des questions secrètes

Il y a enfin ces infos que nous livrons publiquement sur les réseaux sociaux alors qu'elles contiennent parfois les réponses aux questions censées être «secrètes». «Les questions secrètes sont le talon d'Achille des réseaux sociaux, souligne Gérôme Billois. Elles vous permettent d'accéder à vos comptes en cas d'oubli de mot de passe et ce sont toujours les mêmes: Quel est le prénom de votre mère? Quel est votre plat préféré? Or toutes ces infos peuvent être retrouvées facilement sur les réseaux sociaux.»

… et surtout aux données plus évidentes, qui permettent de personnaliser le phishing

Pour les scénarios ci-dessus, qui peuvent avoir le mérite d'attirer l'attention, la probabilité d'utilisation malveillante est pourtant « faible », assure Gérôme Billois. Parallèlement, «nous passons notre temps à livrer des informations hypersensibles», et de façon bien plus directe. Or l'occupation principale des cybercriminels reste les mails de phishing, et ces données les aident à les personnaliser.
«Si le mail est pointu, que c'est votre « bonne » banque qui vous dit qu'elle a remarqué votre passage à telle heure la veille, et que toutes ces infos sont correctes parce que vous avez partagé ces données sur les réseaux sociaux, il y a toutes les chances pour que vous cliquiez sur le lien malveillant.»…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en 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

Original de l’article mis en page : Sans le savoir, vous offrez aux hackers des données invisibles

---

Précautions à prendre avant de se débarrasser du vieux matériel informatique

Précautions à prendre avant de se débarrasser du vieux matériel informatique

---

Lors de la mise au rebut ou de la revente, il est nécessaire de se préoccuper de l'effacement préalable des informations stockées sur tout dispositif comportant un support de stockage (ordinateur, serveur, téléphone, imprimante, clé USB, appareil photo numérique, récepteur GPS).Il est tout aussi important d'appliquer ces règles d'hygiène lors de la réception d'un matériel d'occasion avant sa réutilisation.La méthode choisie pour effacer les informations existantes sur le support informatique obsolète dépend de son niveau de sensibilité et du risque associé (voir Guide technique de l'ANSSI n° 972-1/SGDN/DCSSI). Dans le cas particulier de données ou de matériels protégés par l'instruction générale interministérielle 1300, une procédure stricte doit être appliquée par des personnels habilités. Dans le cas de l'exportation de matériel hors de l'environnement sécurisé de l'entreprise, ou lors d'un transfert interne entre entités ayant des besoins de confidentialité distincts, la mesure la plus sûre reste l'extraction et la destruction physique des supports de stockage, puis leur remplacement lors de la remise en service.Si cette destruction n'est pas envisageable, il existe, pour des composants type PC (comme les disques durs), des logiciels spécialisés destinés à effacer l'intégralité des données stockées. On peut citer le logiciel Blancco, dont la version 4.8 bénéficie d'une Certification de Sécurité de Premier Niveau délivrée par l'ANSSI.

Les imprimantes et photocopieurs multifonctions

Les imprimantes et photocopieurs multifonctions se comportent comme un ordinateur en intégrant souvent un navigateur web, une messagerie électronique, une connectivité Wifi et Ethernet, un accès USB et un disque dur. Le fonctionnement standard de ce type de matériel implique de stocker sur le disque dur les documents à imprimer ou à scanner. Selon vos activités ou votre mission, ce disque dur pourrait stocker des données confidentielles de votre entreprise. Un point d'attention particulier doit être porté sur les contrats de maintenance qui intègrent parfois un accès distant non contrôlé à l'équipement depuis Internet.

L'imprimante ou le photocopieur propose souvent des fonctionnalités de sécurité permettant l'effacement du disque dur ou la suppression des données liées aux impressions, copies, télécopies et numérisations pouvant être enregistrées sur le disque dur. Ce processus d'effacement peut parfois être activé automatiquement après chaque utilisation, ou programmé pour s'exécuter à intervalles spécifiés. Ces fonctionnalités ne garantissent pas toujours un effacement sécurisé des données considérées, et les périphériques de stockages internes et externes devront faire l'objet d'une procédure similaire aux autres équipements informatiques avant le décommissionnement de l'appareil. Attention toutefois, ces composants restent généralement la propriété de la société louant les appareils.

Lors de la réception d'un matériel de ce type, il conviendra de désactiver les fonctionnalités de stockage «dans le cloud» lors du paramétrage initial de l'appareil si celles-ci sont disponibles, et de s'assurer du niveau de mise à jour de l'appareil. Il faudra bien sûr maintenir ce niveau régulièrement afin de limiter l'exposition de son système d'information à des failles éventuellement apportées par cet équipement.

Les autres matériels informatiques

La plupart des matériels modernes intègrent des fonctions de restauration des paramètres d'usine. Il convient a minima de réinitialiser ainsi tout équipement entrant ou sortant de l'entreprise afin de supprimer par exemple certains mots de passes ou autres paramètres de configuration sensibles qui pourraient être stockés sur ces appareils.

Une réinitialisation permet également de se prémunir d'un éventuel piégeage logiciel simple de l'appareil par son précédent propriétaire.

Documentation

• Guide technique n° 972-1/SGDN/DCSSI : Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter.
http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf
• Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale :
http://www.sgdsn.gouv.fr/IMG/pdf/IGI_1300.pdf
• CSPN du logiciel Blancco :
http://www.ssi.gouv.fr/entreprise/qualification/blancco-data-cleaner-version-4-8/

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en 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

Original de l'article mis en page : Bulletin d'actualité CERTFR-2017-ACT-007

RGPD Règlement Européen sur

la Protection des Données : Voici comment être en règle pour 2018

RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle pour 2018

Le GDPR, règlement européen qui renforce le droit des utilisateurs en matière de données personnelles, entrera en vigueur en mai de l'an prochain. D'ici là, 4 actions doivent être menées.

2017 s'annonce chargé pour toutes les entreprises qui collectent et manipulent, de près ou de loin, de la data en provenance de leurs consommateurs. Pour cause, le nouveau règlement européen sur la protection des données personnelles (GDPR) entrera en application le 25 mai 2018. Son objectif est de renforcer les droits des personnes en la matière… et les obligations des entreprises. Voici comment éviter une amende qui sera salée pour les mauvais élèves : 2 à 4% du chiffre d'affaires ou 20 millions d'euros, le montant le plus élevé étant choisi.

Protéger les données personnelles en amont

Commençons par la bonne nouvelle. L'entreprise qui procède à un traitement de données personnelles n'aura plus à remplir de déclaration auprès de la Cnil pour l'en informer, comme elle y est pour l'instant tenue. Ce pilier de la loi « Informatique et liberté » saute.

« Les entreprises doivent 'en échange' se conformer au concept de « privacy by design » érigé par l'article 25 du règlement », explique Matthieu Berguig, avocat spécialisé en droit des nouvelles technologies. Ce concept leur impose de réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service. « Un fabricant d'objets connectés doit donc se poser des questions de base avant de mettre son produit sur le marché : où son stocké les données, par quel protocole de cryptage seront-elles protégées, sont-elles anonymisées… », illustre Matthieu Berguig. Délestée de ce travail de vérification, la Cnil s'évite beaucoup de paperasse… et gagne du temps pour auditer le marché. « On peut être sûrs que les contrôles seront plus nombreux », prévoit Matthieu Berguig.

Nommer un déléguer à la protection des données

La Cnil pourra travailler dans cette perspective main dans la main avec un collaborateur d'un nouveau genre, le délégué à la protection des données (DPD). L'article 37 impose sa nomination dans plusieurs cas de figure : lorsque « le traitement est effectué par une autorité publique ou un organisme public », lorsque le traitement impose « un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque le traitement à grande échelle concerne « les catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10« . Beaucoup d'entreprises sont donc concernées par l'obligation et toutes sont encouragées à en nommer un.

Chargé de faire respecter le règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, le DPD tient un peu du mouton à cinq pattes. Chez les entreprises déjà bien structurées, le « compliance officer », le collaborateur qui s'assure de la conformité de toute décision business à la législation, sera un candidat naturel à ce rôle de DPD. « Pour toutes les autres, il faut trouver la perle rare, un profil juridique capable également de comprendre les problématiques métiers », note Alan Walter, avocat associé chez Walter Billet Avocats.

Tenir un registre de traitement des données

« En 2017, beaucoup d'entreprises vont s'embarquer dans une totale remise à plat de leurs systèmes de traitement des données à caractère personnel », note Alan Walter. Pour cause, l'article 30 impose aux entreprises de plus de 250 salariés de tenir un registre des traitements effectués. Un registre qui comporte, entre autres, le nom et les coordonnées du responsable du traitement, les finalités du traitement, la catégorie de destinataires auxquels les données à caractère personnel ont été ou seront communiqués. « C'est ce registre qui sera consulté par la Cnil lorsqu'elle voudra entrer en action », précise Matthieu Berguig.

L'article 33 impose d'ailleurs à une entreprise qui a subi une violation de données à caractère personnel d'en notifier l'autorité de contrôle. « Seuls les opérateurs télécoms y étaient jusque-là tenus », note Matthieu Berguig.

Créer une base interopérable pour le droit à la portabilité

L'article 20 du règlement aboutit à la création d'un droit à la portabilité des données personnelles. Si un de vos clients vous quitte pour la concurrence, il a le droit de réclamer le transfert de l'intégralité des données le concernant. « Lorsque cela est techniquement possible », précise l'article. « En d'autres termes, lorsque vous passerez d'une boîte mail à une autre, vous aurez théoriquement le droit d'importer tout votre historique de mails », illustre Matthieu Berguig. Une obligation dont la mise en place pourrait être techniquement compliquée dans de nombreux cas.

Alan Walter souligne un autre écueil, juridique celui-ci, en prenant l'exemple de l'un de ses clients, courtier en assurance pour expatriés. « Les données qu'il recueille sont très sensibles car elles concernent le domaine médical. Elles ne peuvent être transmises à n'importe qui, du fait du secret médical. Donc comment doit-il faire ? », s'interroge-t-il. Dans ce cas, il faudrait s'assurer que le destinataire des données offre les garanties nécessaires pour qu'il ne soit pas porté atteinte aux droits des personnes concernées. Problématique d'autant plus épineuse avec des transferts de données qui sont susceptibles d'intervenir vers des opérateurs situés hors de l'Union européenne et donc soumis à des droits différents. Premiers éléments de réponse début mai 2018.

Original de l'article mis en page : Protection des données : voici comment être en règle pour 2018

A Lire aussi :

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 dessins

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

Comment devenir DPO Délégué à la Protection des Données dans le cadre du RGPD, Règlement européen de protection des données ?

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

Entré en vigueur en mai dernier, le Règlement général sur la protection des données impose de nouvelles règles en matière de gestion des données personnelles. Avec l'obligation pour les entreprises de se mettre en conformité avant mai 2018. Ce qui implique une modification des contrats fournisseurs.

Qui est concerné?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne.

Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

Qu'est-ce qu'une donnée à caractère personnel?

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement.

Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel.

Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées.

Quelles obligations pour les entreprises?

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation…), mais aussi les contrats passés avec les fournisseurs et clients sont impactés (voir encadré ci-dessous).

« Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).

Le GRPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilité en fonction de la mainmise de chacun sur les données. Cette notion de coresponsabilité doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs: en effet, le sous-traitant désigné par une organisation pour assurer le traitement des données devient, avec le RGPD, coresponsable de la légalité des traitements. Il sera donc tenu d'informer ses clients et de tenir des registres pour recenser les données, ainsi que d'accepter les audits demandés par son client pour s'assurer de la conformité des traitements.

Les sous-traitants concernés peuvent être, par exemple, l'éditeur d'un CRM en ligne, le routeur d'une campagne d'e-mailing, un service de relation client, etc. Le responsable du traitement, de son côté, doit s'assurer que ses fournisseurs ont pris les mesures nécessaires pour assurer la sécurité des données.

Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement. Quel impact sur les contrats fournisseurs? Pour se mettre en conformité avec le RGPD, les directeurs achats devront veiller à renforcer les contrats passés avec leur fournisseurs…

Le délégué à la protection des données

Le règlement européen consacre la fonction de Délégué à la Protection des Données (DPD ou en anglais DPO) dans les organismes.

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un DPO :

1. s'ils appartiennent au secteur public,
2. si leur activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. si leur activité principale les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

Les responsables de traitement peuvent opter pour un DPO mutualisé ou externe.

Véritable « chef d'orchestre » de la conformité en matière de protection des données, le DPO est chargé :

1. d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
2. de contrôler le respect du règlement et du droit national en matière de protection des données ;
3. de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA ou EIVP) et d'en vérifier l'exécution ;
4. de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

QUI PEUT ÊTRE DPO ?

Le DPO est désigné sur la base de son expertise.

CONSEILS POUR LA MISE EN PLACE DU FUTUR DPO

Compte tenu que jusqu'au 25 mai 2018, ne non respect de la Loi Informatique et Libertés est passible de 5 ans de Prison et jusqu'à 300 000 euros d'amende, nous vous conseillons fortement d'entamer au plus vite les démarches suivantes déclarer un CIL avant le 25 mai 2018 ou désigner un DPO après. Puis :

1. Réaliser ou faire réaliser un indispensable état des lieux (appelé aussi audit) afin d'identifier l'ensemble des traitements de données personnelles et l'ensemble des lieux dans lesquels des données personnelles sont traitées ;
2. Identifier dans la Loi Informatique et Libertés ou dans le RGPD des particularités propres à votre métier qui vous autorise à certains traitements interdits à d'autres activités ou qui nécessiteraient une demande d'autorisation ;
3. Faire une analyse de risque autour des traitements et des données personnelles présentes dans votre établissement. Cette étape indispensable peut être assurée par notre Expert Denis JACOPINI, Certifié ISO 27005 Risk Manager ;
4. Porter au registre l'ensemble des traitements identifiés ;
5. Mettre en conformité les traitements qui ne respectent pas la loi ou le règlement.
6. Suivre régulièrement l'évolution des traitements au sein de l'organisme.

Articles du règlement associés

Article 13 | Article 14 | Article 30 | Article 33 | Article 35 | Article 36 | Article 37 | Article 38 | Article 39 | Article 47 | Article 57

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

DÉSIGNATION N° DPO-15945

Datadock Organisme validé et référencé

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

Contactez-nous

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

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

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

Nous animons des Formations sur le RGPD en individuel ou en groupes

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

Quelques articles sélectionnés par nos Experts :

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

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

Original de l’article mis en page : Le règlement européen de protection des données et les contrats fournisseurs