Quelles tendances en 2017 pour la sécurité du Cloud ?

	Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

Les menaces inhérentes à l'IoT obligeront les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux Etats-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cyberespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entraînant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et revoient le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ».Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSI endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'atout concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de privilèges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises…[lire la suite]

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 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

---

Réagissez à cet article

Original de l'article mis en page : Sécurité du Cloud : quelles tendances en 2017 ? – Globb Security FR

Le RGPD règlement européen de protection des données et les contrats fournisseurs

Le RDPD, règlement européen de protection des données et les contrats fournisseurs

---

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…[lire la suite]

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

---

Réagissez à cet article

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

Que nous réserve la CyberSécurité en 2017 ?

	Que nous réserve la CyberSécurité en 2017 ?

La fin de l'année c'est aussi et surtout la période des bilans. Dans cet article, nous mettrons en évidence les cinq tendances les plus importantes tendances à venir. Qu'elles se maintiennent ou évoluent durant l'année 2017, une chose est sûre, elles risquent de donner du fil à retordre aux professionnels de la cybersécurité.

1 : intensification de la guerre de l'information
S'il y a bien une chose que la cybersécurité nous a apprise en 2016, c'est que désormais, les fuites de données peuvent être motivées aussi bien par la recherche d'un gain financier ou l'obtention d'un avantage concurrentiel que pour simplement causer des dommages dus à la divulgation d'informations privées. À titre d'exemples, le piratage du système de messagerie électronique du Comité National Démocrate (DNC) américain qui a conduit à la démission de Debbie Wassermann Schultz de son poste de présidente ; ou encore, la sécurité des serveurs de messagerie qui a miné la campagne présidentielle américaine de la candidate Hillary Clinton dans sa dernière ligne droite. Il est également inexcusable d'oublier que Sigmundur Davíð Gunnlaugsson, le Premier ministre islandais, a été contraint de démissionner en raison du scandale des Panama Papers.
Les évènements de ce type, qui rendent publiques de grandes quantités de données dans le cadre d'une campagne de dénonciation ou pour porter publiquement atteinte à un opposant quelconque d'un gouvernement ou d'une entreprise, seront de plus en plus fréquents. Ils continueront de perturber grandement le fonctionnement de nos institutions et ceux qui détiennent actuellement le pouvoir.

2 : l'ingérence de l'État-nation
Nous avons assisté cette année à une augmentation des accusations de violations de données orchestrées par des États-nations. À l'été 2015, l'administration Obama a décidé d'user de représailles contre la Chine pour le vol d'informations personnelles relatives à plus de 20 millions d'Américains lors du piratage des bases de données de l'Office of Personnel Management. Cette année, le sénateur américain Marco Rubio (républicain, État de Floride) a mis en garde la Russie contre les conséquences inévitables d'une ingérence de sa part dans les élections présidentielles.
Il s'agit là d'une autre tendance qui se maintiendra.
Les entreprises doivent donc comprendre que si elles exercent ou sont liées de par leur activité à des secteurs dont les infrastructures sont critiques (santé, finance, énergie, industrie, etc.), elles risquent d'être prises dans les tirs croisés de ces conflits.

3 : la fraude est morte, longue vie à la fraude au crédit !
Avec l'adoption des cartes à puces – notamment EMV (Europay Mastercard Visa) – qui a tendance à se généraliser, et les portefeuilles numériques tels que l'Apple Pay ou le Google Wallet qui sont de plus en plus utilisés, les fraudes directes dans les points de vente ont chuté, et cette tendance devrait se poursuivre. En revanche, si la fraude liée à des paiements à distance sans carte ne représentait que de 9 milliards d'euros en 2014, elle devrait dépasser les 18 milliards d'ici 2018.
Selon l'article New Trends in Credit Card Fraud publié en 2015, les usurpateurs d'identité ont délaissé le clonage de fausses cartes de crédit associées à des comptes existants, pour se consacrer à la création de nouveaux comptes frauduleux par l'usurpation d'identité. Cette tendance devrait se poursuivre, et la fraude en ligne augmenter.
Le cybercrime ne disparaît jamais, il se déplace simplement vers les voies qui lui opposent le moins de résistance. Cela signifie, et que les fraudeurs s'attaqueront directement aux systèmes de paiement des sites Web.

4 : l'Internet des objets (IdO)
Cela fait maintenant deux ans que les experts prédisent l'émergence d'un ensemble de risques inhérents à l'Internet des objets. Les prédictions sur la cybersécurité de l'IdO ont déjà commencé à se réaliser en 2016. Cela est en grande partie dû à l'adoption massive des appareils connectés d'une part par les consommateurs, mais aussi par les entreprises. En effet, d'après l'enquête internationale portant sur les décideurs et l'IdO conduite par IDC, environ 31 % des entreprises ont lancé une initiative relative à l'IdO, et 43 % d'entre elles prévoient le déploiement d'appareils connectés dans les douze prochains mois. La plupart des entreprises ne considèrent pas ces initiatives comme des essais, mais bien comme faisant partie d'un déploiement stratégique à part entière.
Cette situation va considérablement empirer. L'un des principaux défis de l'IdO n'est pas lié à la sécurisation de ces appareils par les entreprises, mais plutôt au fait que les fabricants livrent des appareils intrinsèquement vulnérables : soit ils sont trop souvent livrés avec des mots de passe par défaut qui n'ont pas besoin d'être modifiés par les utilisateurs, soit la communication avec les appareils ne requiert pas une authentification de niveau suffisant ; ou encore, les mises à jour des firmwares s'exécutent sans vérification adéquate des signatures. Et la liste des défauts de ces appareils n'en finit pas de s'allonger.
Les entreprises continueront d'être touchées par des attaques directement imputables aux vulnérabilités de l'IdO, que ce soit par des attaques par déni de service distribué (attaques DDoS), ou par le biais d'intrusions sur leurs réseaux, rendues possibles par les « faiblesses » inhérentes de l'IdO.

5 : bouleversements de la réglementation…[lire la suite]

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 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

---

Réagissez à cet article

Original de l’article mis en page : Les grandes tendances 2017 de la cybersécurité, Le Cercle

---

Le Règlement Général sur la Protection des Données (RGPD) en détail

	Le Règlement Général sur la Protection des Données (RGPD) en détail

---

Après quatre années d'âpres négociations, les États Membres de l'Union Européenne sont enfin convenus d'un texte venant moderniser la directive 1995/46/CE du 24 octobre 1995, laquelle datait des débuts d'Internet. Mais, contrairement à une directive, le Règlement adopté le 8 avril 2016 par le Conseil de l'Europe puis, le 16 avril, par le Parlement européen, est d'application directe et s'imposera aux États Membres à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales.

Le processus d'élaboration du texte, long et émaillé de près de 4000 amendements, a mis au monde un texte très long – plus de 200 pages – comportant 99 articles introduits par 173 considérants.
Intitulé *« Règlement n°2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »*, le texte résultant, complexe et technique, est particulièrement difficile à aborder par les entreprises et les administrations, lesquelles sont pourtant les principaux acteurs visés par le texte. Ainsi, dans un article du 18 octobre 2016, le journal La Tribune écrivait que *« 96% des entreprises des trois principales économies européennes [France, Allemagne, Royaume-Uni] ne comprennent pas encore clairement le Règlement général de protection des données (RGPD) (…) Selon une étude publiée ce mardi par la société de sécurité informatique Symantec, 92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD »* !
Les acteurs du traitement de données vont donc devoir investir considérablement pour se mettre à niveau de la nouvelle réglementation, d'autant que toutes les entreprises du monde traitant des données personnelles de citoyens européens sont concernées par le Règlement.
Nous nous proposons, à travers cet article, d'exposer les principales nouveautés du texte sous une forme compréhensible pour le non-initié. Nous dresserons au préalable un tableau général des intentions du texte (I) avant d'insister sur ses innovations principales (II).

I- Présentation générale du RGPD
Le but déclaré du texte est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles, tout en simplifiant, en l'unifiant, la réglementation pour les entreprises.
Les citoyens pourront désormais réclamer contre l'utilisation abusive de leurs données auprès d'une autorité unique, chargée de la protection des données, plutôt que de devoir le faire auprès de l'entreprise détentrice de leurs données. Les particuliers pourront également se joindre à des recours collectifs via des organisations représentatives qui, si la loi nationale les y autorise, pourront agir de leur propre initiative.
Le RGPD développe ainsi considérablement les droits reconnus à la personne dont les données sont collectées. Ainsi, des trois droits reconnus à la personne par la loi Informatique et Liberté (opposition au traitement sous réserve de motif légitime, droit d'accès/communication aux données, droit de rectification/suppression), l'on passe à 11 droits (droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité des données, droit d'opposition (notamment au profilage), etc …). D'une manière générale, la personne concernée dispose d'un droit étendu et facilité à accéder aux données à caractère personnel qui la concernent et le texte réaffirme les principes essentiels de la protection de la vie privée :
• Restriction d'utilisation ;
• Minimisation des données ;
• Précision ;
• Limitation du stockage ;
• Intégrité ;
• Confidentialité.
Les entreprises sont incitées à privilégier l'utilisation de pseudonymes avant et pendant le traitement des données pour en garantir la protection (concept de la prise en compte du respect de la vie privée dès la conception). La « *pseudonymisation* » consiste à s'assurer que les données sont conservées sous une forme ne permettant pas l'identification directe d'un individu sans l'aide d'informations supplémentaires.

II- Principales mesures du RGPD

1. Réalisation d'une analyse d'impact avant la mise en place d'un traitement de données
Avant la mise en place d'un traitement de données pouvant présenter des risques pour la protection des données personnelles, l'entreprise devra réaliser une analyse d'impact : « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* » (Article 35 du Règlement)
Le RGPD introduit ainsi le concept de prise en compte du respect de la vie privée dès la conception du traitement : les différentes obligations pesant sur la collecte des données doivent être prises en compte dès la conception du traitement de données (« *privacy by design and by default* »).

2. Consentement clair et explicite à la collecte des données
La directive 1995/46/CE donnait une définition du consentement à la collecte des données, laquelle a été transposé de manière très hétérogène dans les législations nationales, certaines exigeant un consentement explicite, d'autres décidant qu'un consentement implicite était suffisant. Notre loi Informatique et Liberté se contente ainsi de définir des cas dans lesquels le consentement devrait être explicite. Le Règlement vient unifier une fois pour toute cette définition au onzième point de son article 4 consacré aux définitions, en définissant le consentement comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».
Ce consentement doit donc être express. Il doit résulter d'un acte positif. La personne doit réellement avoir été mise devant la nécessité de donner son accord au traitement. Ainsi, dans son considérant n°32, le Règlement précise qu' « *il ne saurait dès lors y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité.* » Plus encore, la charge de la preuve du consentement pèse sur le responsable du traitement (article 7, 1°). En outre, la personne dont les données sont collectées peut retirer son consentement à tout moment (article 7, 3°).
Malgré cela, le Règlement prévoit un certain nombre de cas pour lesquels le traitement demeure licite même sans consentement (article 6, b) à f)) :
• Lorsque ce traitement est nécessaire à l'exécution d'un contrat accepté par la personne ;
• Lorsque le traitement découle d'une obligation légale ;
• Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ;
• Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
• Tout autre intérêt légitime du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne, en particulier s'il s'agit d'un enfant.

3. Accès facilité de la personne à ses données
Les personnes dont les données sont collectées disposent de droits à la rectification, à l'effacement des données et à l'oubli : « *la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données la concernant et le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais* » (Article 17), et ce pour six motifs : les données ne sont plus nécessaires, la personne concernée retire son consentement, la personne concernée s'oppose au traitement à des fins de prospection, les données ont fait l'objet d'un traitement illicite, les données doivent être effacées pour respecter une obligation légale, ou encore les données ont été collectées dans le cadre d'une offre de service à destinations de mineurs.

4. Notification des violations de données personnelles (« Data Breach Notification »)
A l'heure actuelle, les différentes directives européennes font peser sur les entreprises du secteur de la télécommunication l'obligation d'informer les autorités en cas « *d'accès non autorisé* » à des données personnelles. En clair, lors d'un piratage. Le Règlement, quant à lui, généralise cette obligation de signalement à l'ensemble des responsables de traitement, en ce compris leurs sous-traitants, et ce au plus tard 72 heures après la découverte du problème (Article 33). Bien entendu, il faut que le problème atteigne une certaine gravité pour qu'il soit nécessaire de le rapporter, et tout va donc dépendre de la détermination du seuil à partir duquel le signalement devient obligatoire. L'article 34 du Règlementindique que ce signalement devra intervenir « *lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.* » L'emploi du mot « *élevé* » laisse donc place à appréciation et donnera donc probablement lieu au développement d'une jurisprudence abondante.
Les personnes concernées par la violation des données doivent également être notifiées dans les meilleurs délais, sauf si des mesures de protection ont été mises en œuvre ou seront prises ultérieurement.

5. La création et la maintenance d'un registre des traitements devient obligatoire
Aux termes de l'article 30 du RGPD, un registre détaillé des traitements doit désormais être obligatoirement conservé non seulement par le responsable du traitement mais également par ses éventuels sous-traitants. Ce registre doit pouvoir être mis à tout moment à disposition des autorités de contrôle.
Le texte insiste ainsi sur la responsabilité du contrôleur des données, lequel est responsable de la conformité du traitement avec le Règlement et doit être, à tout moment, en mesure de la démontrer.
Lorsque le traitement de données est délégué par le responsable du traitement à un sous-traitant, ou « *data processor* », même situé hors de l'Union Européenne, celui-ci a désormais les mêmes obligations que le responsable du traitement, y compris la désignation d'un délégué à la protection des données, et ce même dans le cas d'un traitement de données gratuit.

6. Création des délégués à la protection des données (Data Protection Officer)
Si notre loi Informatique et Liberté, et ses mises à jour, ont créé le Correspondant Informatique et Liberté (le « *CIL* »), le Règlement, quant à lui, rend obligatoire dans certains cas la nomination d'un délégué à la protection des données (DPD ou, en anglais, DPO : Data Protection Officer) pour les organismes privés ou publics dont « *les activités de base (…) exigent un suivi régulier et systématique à grande échelle des personnes concernées* » ou lorsque « *le traitement est effectué par une autorité publique ou un organisme public* » (article 37), à l'exception des juridictions. Ce délégué n'est obligatoire que dans certains cas, mais il est fortement recommandé de le nommer systématiquement puisque toute entreprise ou administration doit être capable à tout moment de rendre comptes à l'autorité de contrôle de l'état de ses traitements de données.
Le rôle du délégué à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le RGPD, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de surveillance.

7. Le transfert des données est soumis à vérification et peut être demandé par la personne elle-même
Les transferts de données personnelles vers des pays étrangers sont désormais soumis à la vérification des garanties offertes par les lois de ce pays pour préserver un niveau de sécurité équivalent pour les données. L'article 45 du Règlement prévoit que, dans l'idéal, le pays destinataire devra être listé par la Commission européenne. A défaut, des clauses de garantie spéciales devront être prévues dans les contrats, outre la possibilité de recourir à des codes de conduite, des certifications et autres labels. Auquel cas, il ne sera pas nécessaire d'obtenir une autorisation auprès de l'autorité nationale du pays d'origine des données.
En outre, l'article 49 du Règlement prévoit que, si le traitement nécessitait de recueillir le consentement de la personne, alors celle-ci devra être informée du transfert de ses données et des risques que présentent l'opération. Ceci, bien entendu, afin de permettre à la personne de revenir éventuellement sur son consentement.
Enfin, les personnes dont les données sont collectées disposent elles-mêmes d'un droit à demander le transfert des données les concernant (ou « *droit à la portabilité des données* ») vers un autre fournisseur de services : « *Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* » (Article 20).

8. Restriction du profilage automatisé servant de base à une décision
L'article 21 du Règlement dispose que « *La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* », sauf si ce traitement est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou bien que la décision est autorisée par le droit de l'Union européenne, ou bien encore que le consentement explicite de la personne concernée a été recueilli en amont.

9. Recours et aggravation considérable des sanctions
La directive 1995/46/CE prévoyait jusqu'ici simplement la possibilité, pour la personne dont les droits ont été violés, de recourir aux tribunaux et d'obtenir du responsable du traitement réparation de son préjudice.
Le Règlement prévoit quant à lui un « *droit à un recours effectif* » (articles 78 et 79) et un « *droit à réparation* » (article 82). Il définit des règles de compétences des juridictions se substituant aux règles de droit international privé des États Membres et détermine les amendes qui devront être délivrées par les autorités nationales de contrôle (article 83). Or, les amendes mises en place par le Règlement sont considérables, puisqu'elles peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial ! Le risque qui pèse sur les entreprises imprudentes est donc très sérieux…[lire la suite]

Notre métier :
Nous proposons des service d'accompagnement sur plusieurs niveaux :
1/ Au niveau des utilisateurs qui, face à la résistance au changement, doivent comprendre l'intérêt des démarches de mise en conformité des traitements des données personnelles, pour favoriser leur implication et faciliter la mission du Correspondant aux Données Personnelles.
1'/ Au niveau des utilisateurs encore pour sensibiliser les utilisateurs aux différentes formes d'attaques et d'arnaques informatiques (cybercriminalité) dont les établissements sont très largement victimes.
Les services chargés de gérer les fournisseurs sont fortement incités à suivre notamment un module sur les arnaques aux FOVI et à voir leurs procédures auditées et probablement améliorées.
2/ Au niveau de l'établissement complet afin de faire un état des lieux des traitements concernés et un audit des mesures de sécurité en place et à faire évoluer pour les rendre acceptables vis à vis de la Réglementation relative aux Données Personnelles.
3/ Au niveau du futur CIL ou du futur DPO afin de lui faire découvrir ses misions, l'accompagner dans sa prise de fonction et l'accompagner au fil des changements.

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

---

Réagissez à cet article

Original de l’article mis en page : RGPD : le Règlement Général sur la Protection des Données qui bouleverse la loi Informatique et Liberté. Par Bernard Rineau, Avocat, et Julien Marcel, Juriste.

Devenir délégué à la protection des données | CNIL

	Comment devenir délégué à la protection des données (DPD ou DPO)

Le délégué à la protection des données (D.P.D.) ou Data Protection Officer (D.P.O.) est au cœur du nouveau règlement européen. Les lignes directrices adoptées le 13 décembre 2016 par le G29, groupe des « CNIL » européennes, clarifient et illustrent d'exemples concrets le nouveau cadre juridique applicable en mai 2018 dans toute l'Europe.

Le règlement européen sur la protection des données pose les règles applicables à la désignation, à la fonction et aux missions du délégué, sous peine de sanctions.

Les lignes directrices du G29 ont pour objectif d'accompagner les responsables de traitement et les sous-traitants dans la mise en place de la fonction de délégué ainsi que d'assister ces délégués dans l'exercice de leurs missions. Elles contiennent des recommandations et des bonnes pratiques permettant aux professionnels de se préparer et de mettre en œuvre leurs obligations avec flexibilité et pragmatisme.

A retenir
Le délégué est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné.
Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.

Pour garantir l'effectivité de ses missions, le délégué :
• doit disposer de qualités professionnelles et de connaissances spécifiques,
• doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.
La mise en place de la fonction de délégué nécessite d'être anticipée et organisée dès aujourd'hui, afin d'être prêt en mai 2018.

Dans quels cas un organisme doit-il obligatoirement désigner un délégué à la protection des données ?

La désignation d'un délégué est obligatoire pour :
1. Les autorités ou les organismes publics,
2. Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations.

En dehors des cas de désignation obligatoire, la désignation d'un délégué à la protection des données est encouragée par les membres du G29. Elle permet en effet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles.
Les organismes peuvent désigner un délégué interne ou externe à leur structure. Le délégué à la protection des données peut par ailleurs être mutualisé c'est-à-dire désigné pour plusieurs organismes sous certaines conditions. Par exemple, lorsqu'un délégué est désigné pour un groupe d'entreprises, il doit être facilement joignable à partir de chaque lieu d'établissement. Il doit en effet être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec l'autorité de contrôle.
Les lignes directrices du G29 clarifient les critères posés par le règlement, notamment les notions d'autorité ou d'organisme public, d'activités de base, de grande échelle et de suivi régulier et systématique.

Qui peut être délégué à la protection des données ?

Le délégué est désigné sur la base de ses qualités professionnelles et de sa capacité à accomplir ses missions.
Le délégué doit posséder des connaissances spécialisées de la législation et des pratiques en matière de protection des données. Une connaissance du secteur d'activité et de l'organisme pour lequel il est désigné est également recommandée. Il doit enfin disposer de qualités personnelles, et d'un positionnement lui donnant la capacité d'exercer ses missions en toute indépendance.
Les lignes directrices du G29 précisent le niveau d'expertise, les qualités professionnelles et les capacités du délégué.
Les personnes désignées en tant que correspondant Informatique et Libertés (CIL) ont vocation à devenir délégués à la protection des données en 2018. Toutefois, la qualité de CIL n'ouvrira pas automatiquement droit à celle de délégué à la protection des données. Les organismes ayant désigné un CIL indiqueront à la CNIL en 2018 si leur CIL deviendra délégué à la protection des données, selon des modalités précisées ultérieurement.

Quelles sont les missions du délégué à la protection des données ?

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :
• **d'informer et de conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
• **de contrôler le respect du règlement** et du droit national en matière de protection des données ;
• **de conseiller l'organisme** sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
• **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci.
Les lignes directrices détaillent le rôle du délégué en matière de contrôle, d'analyse d'impact et de tenue du registre des activités de traitement.
Elles indiquent que **le délégué n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement**.

Quels sont les moyens d'action du délégué à la protection des données ?

Le délégué doit bénéficier du soutien de l'organisme qui le désigne. L'organisme devra en particulier :
• **s'assurer de son implication** dans toutes les questions relatives à la protection des données (exemple : communication interne et externe sur sa désignation)
• **lui fournir les ressources nécessaires** à la réalisation de ses tâches (exemples : formation, temps nécessaire, ressources financières, équipe)
• **lui permettre d'agir de manière indépendante** (exemples : positionnement hiérarchique adéquat, absence de sanction pour l'exercice de ses missions)
• **lui faciliter l'accès aux données et aux opérations de traitement** (exemple : accès facilité aux autres services de l'organisme)
• **veiller à l'absence de conflit d'intérêts.**
Les lignes directrices fournissent des exemples concrets et opérationnels des ressources nécessaires à adapter selon la taille, la structure et l'activité de l'organisme. S'agissant du conflit d'intérêts, le délégué ne peut occuper des fonctions, au sein de l'organisme, qui le conduise à déterminer les finalités et les moyens d'un traitement (ne pas être juge et partie). L'existence d'un conflit d'intérêt est appréciée au cas par cas. Les lignes directrices indiquent les fonctions qui, en règle générale, sont susceptibles de conduire à une situation de conflit d'intérêts.

Comment organiser la fonction de délégué à la protection des données ?

En vue de la préparation à la fonction de délégué, il est recommandé de :
• s'approprier les nouvelles obligations imposées par le règlement européen, en s'appuyant notamment sur les lignes directrices du G29.
• confier au CIL ou au futur délégué les missions suivantes :
- **réaliser l'inventaire des traitements** de données personnelles mis en œuvre ;
- **évaluer ses pratiques et mettre en place des procédures** (audits, *privacy by design*, notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
- **identifier les risques** associés aux opérations de traitement ;
- **établir une politique de protection des données personnelles** ;
- **sensibiliser les opérationnels et la direction** sur les nouvelles obligations.

Lignes directrices du G29
> Guidelines on Data Protection Officers ('DPOs')
> WP243 ANNEX – Frequently asked questions
La version française de ces documents sera disponible début 2017.

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 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

---

Réagissez à cet article

Original de l’article mis en page : Devenir délégué à la protection des données | CNIL

L’essentiel Online – La surveillance au travail pourrait être modifiée – Luxembourg

	La surveillance au travail pourrait être modifiée

Les députés se sont penchés lundi sur le nouveau cadre concernant la protection des données au Grand-Duché.

Un patron pourrait bientôt ne plus avoir besoin de demander une autorisation préalable à la Commission nationale pour la protection des données (CNPD) avant de placer ses employés sous vidéosurveillance au travail. Cette mesure fait partie d'un projet de loi concernant la protection des données privées que les députés ont commencé à étudier lundi et qui s'inscrit dans le nouveau règlement européen qui entrera en vigueur le 25 mai 2018.

Le texte supprime la liste de traitement des données qui est aujourd'hui soumis à autorisation préalable de la CNPD, dont les traitements effectués à fin de surveillance. La CNPD fera, selon le projet de loi, des contrôles a posteriori, dans un but de simplification administrative. Un changement qui a suscité l'inquiétude de plusieurs députés, soucieux de protéger les citoyens d'une surveillance illégale par leurs employeurs.

La Chambre des salariés avait émis un avis défavorable en novembre, «dénonçant d'emblée la suppression de l'autorisation préalable (…). Elle s'oppose plus particulièrement, et de manière formelle, à cette exemption en faveur des traitements à des fins de surveillance sur le lieu de travail», expliquant que la loi actuelle, de 2002, «traduisait justement la volonté expresse du législateur luxembourgeois de protéger les personnes physiques de certains traitements « susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées »». À noter que le projet de loi introduit également des sanctions financières.
(JW/JV/*L'essentiel*)

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 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

---

Réagissez à cet article

Original de l'article mis en page : L'essentiel Online – La surveillance au travail pourrait être modifiée – Luxembourg

Prévisions cybercriminalité pour 2017

	Prévisions cybercriminalité pour 2017

Nous sommes tombés sur cet article sur le site Internet « Informaticien.be » et n'avons pas pu nous empêcher de le partager avec vous tant il est en accord avec les prévisions ressorties de nos analyses. Aux portes de 2017, les entreprises, administrations et association non seulement vont devoir s'adapter à une réglementation Européenne risquant s'impacter lourdement la réputation des établissements qui devront signaler à la CNIL qu'elle viennent d'être victime de piratage, mais également, l'évolution des techniques de piratage vont augmenter les risques qu'auront les organismes à se faire pirater leurs systèmes informatiques. N'hésitez pas à consulter notre page consacrée aux bons conseils que nous prodiguons depuis de nombreuses années sur https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles.
Denis JACOPINI

Trend Micro présente son rapport annuel des prévisions en matière de sécurité: 'The Next Tier – 8 Security Predictions for 2017'. L'année prochaine sera marquée par des attaques de plus grande envergure à tous les niveaux. Les cybercriminels adopteront des tactiques différentes pour tirer parti de l'évolution du paysage technologique.
« Nous pensons que la General Data Protection Regulation (GDPR) va non seulement changer fondamentalement la manière dont les entreprises gèrent leurs données, mais aussi induire de nouvelles méthodes d'attaque. La tactique du ransomware va également s'étendre pour toucher plus d'appareils, tandis que la cyberpropagande influencera de plus en plus l'opinion publique", déclare Raimund Genes, CTO de Trend Micro.
En 2016, l'on a assisté à une formidable augmentation des vulnérabilités d'Apple avec pas moins de 50 fuites. A cela s'ajoutent 135 bugs Adobe et 76 bugs Microsoft. Alors que Microsoft continue d'améliorer ses facteurs limitatifs et qu'Apple est de plus en plus considéré comme le système d'exploitation prépondérant, ce déplacement apparent des 'exploits' des logiciels vulnérables va encore s'accentuer en 2017.
L'IoT et l'IIoT – dans la ligne de mire des attaques ciblées
L'Internet of Things (IoT – internet des objets) et l'Industrial Internet of Things (IioT – internet industriel des objets) seront de plus en plus dans la ligne de mire des attaques ciblées en 2017. Ces attaques tirent parti de l'engouement croissant suscité par les appareils connectés en exploitant les failles et les systèmes non protégés et en perturbant des processus d'entreprise. L'usage croissant d'appareils mobiles pour surveiller les systèmes de production dans les usines et les milieux industriels, combiné au nombre important de vulnérabilités dans ces systèmes constitue une réelle menace pour les organisations.
Explosion de l'extorsion professionnelle
Le Business E-mail Compromise (BEC) et le Business Process Compromise (BPC) représentent de plus en plus une forme relativement simple et économiquement rentable d'extorsion professionnelle. En incitant un employé innocent à verser de l'argent sur le compte bancaire d'un criminel, une attaque BEC peut rapporter 140.000 dollars. Bien que le piratage direct d'un système de transaction financière exige plus d'efforts, cela représente une manne de pas moins de 81 millions de dollars pouvant tomber aux mains des criminels.
Autres faits marquants du rapport
Le nombre de nouvelles familles de ransomware ne progresse que de 25 %. Mais le ransomware s'étend désormais aux appareils IoT et aux terminaux informatiques autres que les desktops (par exemple les systèmes POS ou les distributeurs automatiques).
Les fournisseurs ne parviendront pas à protéger à temps les appareils IoT et IIoT pour éviter des attaques DoS (refus de service) ou d'autres types d'attaques.
Le nombre de failles découvertes dans les technologies Apple et Adobe augmente, ce qui vient s'ajouter aux « exploit-kits ».
46 pour cent de la population mondiale est aujourd'hui reliée à l'internet : la cyberpropagande ne va cesser d'augmenter, à présent que les nouveaux dirigeants des grands pays sont en place. L'opinion publique risque donc d'être influencée par de fausses informations.
Comme ce fut le cas lors de l'attaque de la Banque du Bangladesh plus tôt cette année, les cybercriminels parviennent à modifier des processus d'entreprise via des attaques BPC, et à en tirer largement profit. Les attaques BEC restent d'actualité pour extorquer des fonds à des employés qui ne se doutent de rien.
Le GDPR produira des changements de politique et administratifs qui auront un lourd impact sur les coûts. Cela exigera aussi des examens complexes des processus de données pour assurer la conformité réglementaire.
De nouvelles méthodes d'attaques ciblées déjoueront les techniques de détection modernes, permettant aux criminels de s'attaquer à différentes organisations.
Original de l'article mis en page : Le ransomware s'étend aux appareils connectés et à l'internet des objets – Press Releases – Informaticien.be

---

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 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

---

Réagissez à cet article

Original de l’article mis en page : Le ransomware s’étend aux appareils connectés et à l’internet des objets – Press Releases – Informaticien.be

---

Ce que les entreprises doivent savoir pour se mettre en conformité avec Règlement européen de protection des données en vigueur dans 18 mois

	Ce que les entreprises doivent savoir pour se mettre en conformité avec Règlement européen de protection des données en vigueur dans 18 mois

---

Entré en vigueur en mai 2016, le RGPD (Règlement général sur la protection des données) modifie les règles de gestion des données à caractère personnel dans les entreprises. Fin mai 2018, toutes les organisations devront être en conformité. Il vous reste donc moins de 18 mois pour mener ce chantier.

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. À noter, le RGPD prévoit des exceptions selon les traitements concernés, notamment au niveau des traitements de données RH (recrutement, contrat de travail…), pour lesquels les États membres peuvent prévoir « des règles plus spécifiques pour assurer la protection des droits et libertés » (article 88).

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 sous-traitants et clients sont impactés. « 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.

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 (voir encadré en page suivante)…[lire la suite]

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 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

---

Réagissez à cet article

Original de l’article mis en page : Règlement européen de protection des données: les nouvelles règles de gestion des données

---

Les jouets connectés s’amusent avec nos données personnelles

	Les jouets connectés s’amusent avec nos données personnelles

---

Une étude technique menée par plusieurs associations de défense des consommateurs dénonce les failles de sécurité et les CGU de plusieurs jouets connectés.

À seulement quelques semaines de Noël, l'association de défense des consommateurs UFC-Que Choisir part en croisade contre les jouets connectés. Cette étude, faite de concert avec l'association norvégienne Forbrukerradet s'attarde sur deux jouets en particulier : la poupée Cayla et le robot i-Que.

Une connexion Bluetooth vulnérable

Sont tout d'abord dénoncées des failles de sécurité qui entourent le protocole Bluetooth. La connexion entre les jouets et le smartphone se fait sans aucun code d'accès. Étant donné qu'ils sont munis d'un micro, un tiers se situant à moins de 20 mètres peut s'y connecter et entendre les échanges avec l'enfant. Il pourrait même prendre le contrôle total du jouet.

La protection des données personnelles passe à la trappe

L'UFC-Que choisir s'en prend aussi la sécurité des données personnelles. Malgré la loi « Informatique et libertés », les conditions contractuelles autorisent la collecte des données vocales. « *Ces données peuvent ensuite être transmises, notamment à des fins commerciales, à des tiers non identifiés. Les données sont aussi transférées hors de l'Union européenne, sans le consentement des parents* » explique l'UFC.

Enfin pour couronner le tout, ces jouets font du placement produit : »*l'étude a ainsi révélé que Cayla et i-Que prononcent régulièrement des phrases préprogrammées, faisant la promotion de certains produits – notamment des produits Disney ou des références aux dessins animés de Nickelodeon*« . L'association de consommateur a donc décidé de saisir la CNIL afin qu'elle contrôle le respect de la protection de données personnelles, ainsi que la DGCCRF pour qu'elle sanctionne les manquements aux dispositions légales et réglementaires sur la sécurité.

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 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

---

Réagissez à cet article

Original de l'article mis en page : L'UFC-Que Choisir épingle les jouets connectés sur la sécurité des données personnelles – CNET France

Les collectivités territoriales aussi concernées par la cybersécurité

Les collectivités territoriales aussi concernées par la cybersécurité

Pour mieux appréhender la transition numérique, les écoles de Saint-Cyr Coëtquidan organisent un colloque régional destiné aux collectivités territoriales,
Trois questions à…
Gérard de Boisboissel, ingénieur au centre de recherche des écoles Saint-Cyr Coëtquidan, organisateur du colloque.

En quoi la cybersécurité concerne les collectivités territoriales ?
La transformation numérique touche tout le monde, donc la protection des données aussi. Il y a des enjeux et des risques, les petites communes comme la région sont vulnérables car elles détiennent des données personnelles.

Quels types d'attaques sont les plus fréquentes ?
On observe plusieurs types d'attaques : le piratage ou cryptage de données mais aussi une prise de contrôle des sites Internet par des hackers. En janvier 2015, plusieurs sites bretons, dont celui de la mairie de Port-Louis (56), ont été piratés et présentaient une page d'accueil avec un message islamiste.

Comment se protéger ?
Si toutes les collectivités territoriales sont conscientes de la transformation numérique, les élus n'avancent pas tous au même rythme. Pendant le colloque, nous aborderons les bons réflexes à adopter : sauvegarder ses données en double, changer ses mots de passe régulièrement, et pourquoi pas désigner une personne dédiée à cette question. Vannes apportera son témoignage demain, car la ville a un référent cybersécurité et consacre 25 000 € à ce sujet…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Vannes. Les petites communes aussi concernées par la cybersécurité