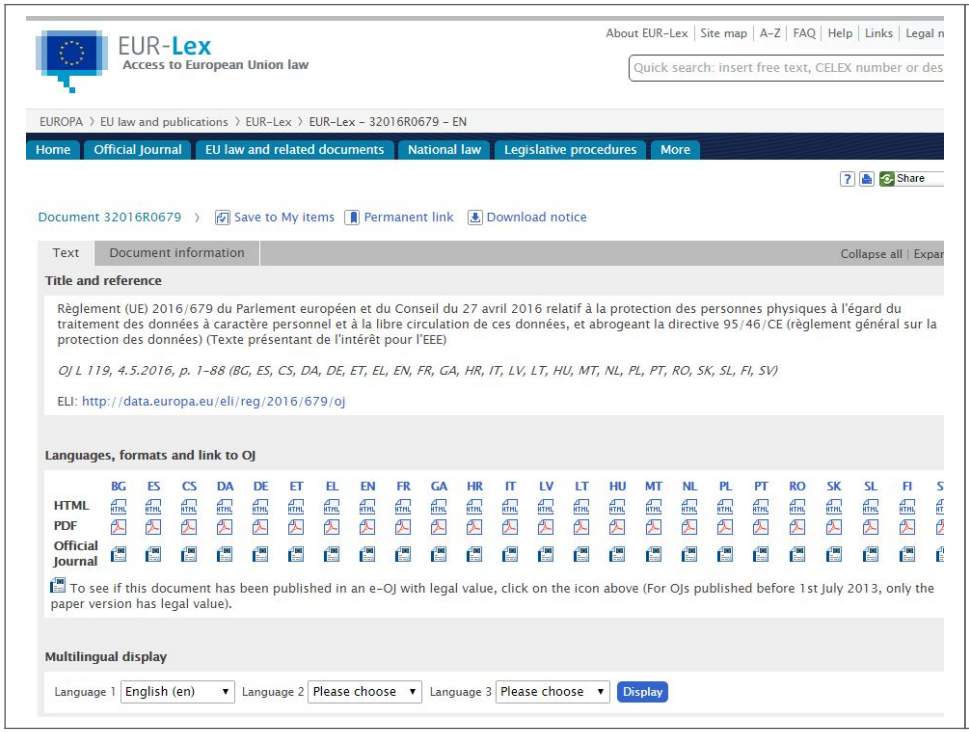
Introduction au Règlement Européen sur la Protection des Données



Introduction au Règlement Européen sur la Protection des Données

Le Règlement Général de l'Union Européenne sur la Protection des Données (RGPD) impose aux entreprises d'effectuer un suivi de toutes les occurrences des données à caractère personnel des clients au sein de leur organisation, d'obtenir le consentement des clients concernant l'utilisation de leurs informations personnelles (y compris le « droit à l'oubli ») et de documenter l'efficacité de cette gouvernance des données pour les auditeurs.

Deux tiers (68 %) des entreprises, selon Compuware, risquent de ne pas être en conformité avec le RGPD, en raison d'une augmentation de la collecte des données, de la complexité informatique grandissante, de la multiplicité des applications, de l'externalisation et de la mobilité. Ce risque tient aussi aux politiques laxistes concernant le masquage des données et l'obtention d'une autorisation explicite des clients en matière de données. Les entreprises européennes comme américaines doivent, par conséquent, adopter une série de bonnes pratiques, notamment un masquage plus rigoureux des données de test et de meilleurs pratiques concernant le consentement des clients, afin d'éviter des sanctions financières et une altération possible de leur image de marque résultant d'une non-conformité.
Le RGPD de l'Union européenne a été adopté en avril 2016, afin d'unifier des obligations auparavant réparties à travers différentes juridictions européennes concernant l'utilisation, la gestion et la suppression des informations personnellement identifiables (IPI) des clients par les entreprises. Toutes les entreprises dans l'UE, aux États-Unis et ailleurs, qui collectent des IPI relatives à des citoyens de l'UE, ont jusqu'en mai 2018 pour se conformer à ces dispositions. Tout non-respect du RGPD expose les entreprises à des amendes pouvant atteindre 20 millions € ou 4 % du chiffre d'affaires mondial….[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Retour sur le RGPD, le Règlement Général de l’Union Européenne sur la Protection des Données – Data Security BreachData Security Breach

---

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

---

En proposant de nouvelles règles télécom cette semaine, la Commission européenne introduirait des obligations de sécurité aux services de messagerie. Des obligations déjà en vigueur pour les opérateurs, qui réclament une parité réglementaire avec les acteurs en ligne.

Équilibrer les obligations entre opérateurs et messageries en ligne ressemble souvent à un travail de funambule, dans lequel se lancerait la Commission européenne. Dans quelques jours, l'institution doit dévoiler une révision des règles télécoms en Europe. Selon un brouillon obtenu par Reuters, elle y introduirait des obligations de sécurité pour les services de messagerie en ligne, déjà appliquées par les opérateurs.

Des obligations de signalement des brèches

À la mi-août, plusieurs médias affirmaient que la Commission européenne comptait proposer cette parité entre acteurs. Le brouillon obtenu par Reuters viendrait donc confirmer cette piste. Dans celui-ci, les services « over the top » devront ainsi signaler les brèches « *qui ont un impact important sur leur activité* » aux autorités et disposer d'un plan de continuité de l'activité. Les services qui proposent des numéros de téléphone ou d'en appeler, comme Skype, devront aussi permettre les appels d'urgence.

Pourtant, ces règles pourront être plus légères pour ces services que pour les opérateurs classiques, dans la mesure où les services ne maîtrisent pas complètement la transmission des contenus via les tuyaux. Dans l'absolu, ces règles doivent réduire l'écart d'obligations entre les acteurs télécoms et ceux d'Internet, avec en toile de fond le combat entre des acteurs européens et des sociétés principalement américaines.

Rappelons que le règlement sur les données personnelles, voté en avril par le Parlement européen, doit lui aussi obliger les services à divulguer aux autorités les fuites de données, dans un délai court. En France, cette obligation ne concerne que les opérateurs.

Le moment est d'ailleurs pour celle-ci, le secteur télécom étant notamment le théâtre de lobbyings intenses. Elle a d'ailleursretiré une proposition de « fair use » pour la fin des frais d'itinérance il y a quelques jours, suite à des levées de bouclier du côté des associations de consommateurs, des opérateurs et des eurodéputés. Comme le rappelle Reuters, ce texte passera entre les mains du Parlement et du Conseil de l'Europe, avec des changements possibles à la clé…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**.

Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : L’UE préparerait l’extension de règles de sécurité des opérateurs aux acteurs du Net

---

Protection des données personnelles, plus que quelques mois pour se mettre en règle…

Il y a urgence à se former aux nouvelles obligations en matière de protection des données… Après 4 années de négociations très médiatisées, le nouveau règlement européen de protection des données a été adopté en mai 2016. Il sera applicable en France le 25 mai 2018. Mais une bonne moitié des organisations françaises ne sont toujours pas informées du contenu de la réforme concernant la protection des données.

Pourtant, il y a de vraies conséquences en termes de responsabilités et de sanctions ! En cas de violation des dispositions du règlement, les pénalités peuvent atteindre un montant maximal de 4% du CA mondial d'un groupe ou de 20 Millions d'euros.

De plus, tout organisme public ou privé victime d'un piratage, d'une faille de sécurité ou de tout acte risquant de compromettre ou ayant compromis la sécurité (confidentialité, intégrité) de données personnelles aura 72 heures pour signaler l'incident à la CNIL.
L'organisme devra, dans la plupart des cas informer les victimes (comme Orange a été obligé de le faire à deux reprise en 2014).
Pas bon pour l'image ça !
Imaginez, des années pour construire votre réputation et en quelques heures :
1. Vous devez signaler à la CNIL que vous vous êtes fais pirater et que des données personnelles ont été compromises ;
2. Vous allez très probablement avoir droit à un contrôle de la CNIL qui va venir rechercher la cause de cette faille et par la même occasion faire le point sur votre mise en conformité ;
3. Pour couronner le tout (le 3ème effet Kiss Cool), vous risquez d'informer vos clients, salariés, fournisseurs que leurs données personnes ont été piratées sur votre système informatique. Imaginez leur réaction !!! Toujours pas bon pour l'image ça !

La première étape pour se mettre en conformité est de s'informer et de sensibiliser le personnel qui a un rôle important à jouer dans cette mise sur rail.
Ensuite, il sera nécessaire de former une personne en particulier dans votre établissement. Actuellement il s'appellera CIL (Correspondant Informatique et Libertés), demain DPO (Délégué à la Protection des Données), cette personne va jouer un rôle clé dans votre mise en conformoté.
Il devra :
1. Contrôler le respect du règlement ;
2. Informer et conseiller le responsable du traitement (ou le sous-traitant en charge de cette mission) et les employés qui procèdent au traitement des données sur les obligations qui leur incombent.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Directive NIS adoptée: quelles conséquences pour les entreprises?

Directive NIS depuis juillet. Des changements pour les entreprises?

En juillet dernier, le Parlement européen a adopté la directive NIS (Network and Information Security). Les opérateurs de services ainsi que les places de marché en ligne, les moteurs de recherche et les services Cloud seront soumis à des exigences de sécurité et de notification d'incidents.

C'est fait ! La directive NIS a été approuvée le 6 juillet par le Parlement européen en seconde lecture, après avoir été adoptée en mai dernier par le Conseil de l'Union européenne. Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.

Sécuriser les infrastructures

Du côté des fournisseurs de services numériques, les places de marché en ligne, les moteurs de recherche et les fournisseurs de services de Cloud actifs dans l'UE sont concernés. Ils devront prendre des mesures pour « assurer la sécurité de leur infrastructure » et signaler « les incidents majeurs » aux autorités nationales. Mais les exigences auxquelles devront se plier ces fournisseurs, seront moins élevées que celles applicables aux opérateurs de services essentiels.

Publication de la Directive NIS au Journal officiel de l'Union européenne
Adoption de la directive NIS : l'ANSSI, pilote de la transposition en France

---

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Directive NIS adoptée: quelles conséquences pour les entreprises?

Comment se passera le passage du CIL au DPO lors de la mise en application du RGPD ?

	Comment se passera le passage du CIL au DPO lors de la mise en application du RGPD ?

Plus de vingt ans après la Directive sur la Protection des Données, l'Union Européenne s'est dotée ce printemps d'un nouveau règlement. Les deux décennies passées ont vu des changements phénoménaux dans nos usages du numérique. Le texte, issu d'un délicat compromis entre les institutions européennes et les acteurs du numérique, prend acte de ces changements (en entérinant par exemple le célèbre « droit à l'oubli ») et trace le futur de la protection des données en Europe, notamment en mettant au centre de son texte un acteur nouveau, ou en tout cas ré-inventé, le Data Protection Officer (DPO). Mais au « jour J » de l'entrée en application du texte, qui seront les DPO ? Quelles seront leurs missions, et comment s'y préparer dès maintenant ?

Le DPO, un « CIL 2.0 » ?

Le texte en français (pas encore officiel) du futur règlement européen ne traduit pas, à raison, « Data Protection Officer » par « Correspondant Informatique & Libertés », mais par « Délégué à la protection des données ». En effet, les futurs DPO auront des responsabilités plus diverses que les CIL, mais aussi plus lourdes. Les enjeux sont importants, puisque la CNIL, comme tous ses équivalents européens, pourra, grâce au nouveau règlement, imposer des sanctions financières équivalentes à ce que l'on peut observer en droit de la concurrence (jusqu'à 4 % du chiffre d'affaires annuel mondial). En termes de position, le DPO gagne également en reconnaissance, puisque le règlement stipule que « le délégué à la protection des données fait directement rapport au niveau le plus élevé du responsable de traitement ». Son identité devra également être rendue publique, à l'instar des responsables de l'accès aux documents administratifs désignés au titre de la loi CADA.

Cette montée en responsabilité, interne aussi bien qu'auprès du public, s'accompagnera vraisemblablement d'une hausse des salaires, pour rejoindre ceux que l'on observe en Amérique du Nord, par exemple, où une société dont la réputation fut salie par une affaire de data breach n'a pas hésité à rémunérer ensuite son nouveau CPO à hauteur de 700.000 $ par an pour regagner la confiance de ses clients.

La principale évolution entre CIL et DPO, cependant, demeure dans l'étendue de leur champ d'action. Aux tâches déjà accomplies par le CIL s'ajoutent, pour le DPO, celles de notification et d'enregistrement des violations de données personnelles, ainsi que des analyses d'impact de ces violations, entre autres.

Du CIL au DPO : une transition légitime

Les similarités entre CIL et DPO sont nombreuses, et les compétences, ainsi que l'expérience, accumulée par les CIL ces dix dernières années seront un formidable atout pour aborder les changements qui s'annoncent. Ainsi, pour capitaliser sur les travaux réalisés par les CIL déjà désignés et pour assurer la diffusion la plus large possible de l'esprit de la loi, l'AFCDP, association qui regroupe les professionnels de la conformité Informatique et Libertés et de la protection des données personnelles, demande que soit ménagée une « clause du grand-père » qui permettrait à ces CIL qui le souhaitent et qui répondent aux nouvelles exigences d'être maintenus dans leur fonction en tant que DPO. Par ailleurs, la CNIL soutient ce passage « naturel » du CIL au DPO, comme l'a confirmé Edouard Geffray, Secrétaire général de la CNIL devant les 500 CIL réunis fin janvier à l'occasion de la journée mondiale de la protection des données personnelles : *« Nous avons tout intérêt à ce que la plupart d'entre vous soient confirmés en tant que DPO ».*

Cela ne signifie en aucun cas que le milieu professionnel des CIL devrait refuser d'accueillir de nouveaux arrivants. Il en faudra, en effet, par conséquence logique de la multiplication attendue des postes, le DPO étant obligatoire dans de très nombreuses structures. Il faudra donc s'assurer qu'ils bénéficient de la culture de métier forte que les CIL se sont construites ces dernières années. En revanche, ce qu'il convient plutôt d'essayer de minimiser, c'est la possible délocalisation d'une partie des DPO hors de France. En effet, même si le règlement indique que « *Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement* », il est probable que certains grands groupes décident de localiser leur DPO en Grande-Bretagne, en Irlande, aux Pays-Bas ou en Belgique. Le revers de cette harmonisation européenne serait alors un éloignement croissant entre les citoyens et les responsables du traitement de leurs données à caractère personnel.

Deux précieuses années de préparation

Les nouvelles règles, appelées à remplacer celles de notre actuelle loi Informatique et Libertés, seront applicables le 25 mai 2018. Les organismes ayant déjà désignés un CIL ont une longueur d'avance pour préparer la mise en application du règlement. Les deux années qui viennent seront l'occasion de mettre en place de nouveaux chantiers et de nouvelles pratiques qui, de par leurs nouveautés, vont demander du temps et de la préparation. Ainsi des notifications de violation du traitement des données à caractère personnel, qui devra se faire sans délai auprès de la CNIL, et, dans certaines conditions, auprès des personnes concernées. Cet exercice, qui mêle des compétences en communication, en sécurité et en droit, demande une préparation préalable importante, afin de respecter les délais et d'établir rapidement le dialogue entre les différents acteurs, externes aussi bien qu'internes. À ce titre, deux ans ne seront pas de trop pour préparer, former et communiquer avec les collaborateurs réguliers du CIL. Ce dernier peut aussi avoir intérêt à compléter si besoin sa formation, afin de se préparer au mieux à la transition et d'apparaître auprès de ses supérieurs comme solution naturelle pour remplir la fonction de DPO.

Cette préparation, si elle est conséquente, ne sera pas nécessairement solitaire. Outre les documents officiels appelés à approfondir et clarifier certains détails du texte, les CIL pourront s'appuyer sur leur travail mutuel, notamment l'AFCDP, qui dispose d'ores et déjà d'un groupe de réflexion, aussi bien numérique que physique, sur les nouveaux défis apportés par le règlement. Ce travail bénéficiera en outre du réseau CEDPO (*The Confederation of European Data Protection Organisations*, co-fondée par l'AFCDP) qui permet aux CIL français de profiter des expériences et des bonnes pratiques de leurs confrères allemands, espagnols, néerlandais, polonais, irlandais et autrichiens. Enfin, compte tenu du changement d'échelle et de logique qui s'annonce en matière de protection des données à caractère personnel, il est crucial que les organismes qui n'ont pas déjà désigné un CIL le fassent, pour être prêt en 2018 à faire face aux nouvelles exigences.

Article original de Paul-Olivier Gibert

Président de l'AFCDP

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Règlement européen Données personnelles : du CIL au Data Protection Officer, une transition… – Linkis.com

---

Certification des objets

connectés de santé – Web des Objets

	Certification des objets connectés de santé

De l'objet connecté de bien-être à l'objet connecté de santé : une certification qui a du sens

Très répandus sur le marché, les objets connectés de bien-être ont pour vocation de développer un état de satisfaction morale ou physique, sans obligation de mesurabilité ni de résultats cliniques. Les données de bien-être peuvent être observées sur le long terme pour mieux déterminer l'état de santé d'un patient. De nombreux objets connectés de santé sont en développement, afin de fournir des données quantifiables et médicalement fiables. L'usage de ces objets se fait notamment dans un but nommé le « quantified self ». C'est une collaboration entre utilisateurs et fabricants d'outils qui partagent un intérêt pour la connaissance de soi à travers la mesure et la traçabilité de soi. Des objets connectés tels que la balance Polar connectée pour suivre son poids ou le capteur Withings Go permettant de mesurer son activité physique et de suivre ses cycles de sommeil sont des outils qui s'intégrent dans cette démarche.

« La frontière entre les domaines du bien-être et de la santé va s'estomper. L'objectif est que demain, les gens disent que c'est eux qui prennent soin de leur santé, avec l'aide de leur médecin et non plus leur médecin seul. Le patient devient expert, le médecin va devoir le prendre comme un partenaire. »
Cédric Hutchings, PDG de Withings ***(Cahiers IP n°2 : Le corps, nouvel objet connecté)****.*

L'objet connecté de santé en tant que dispositif médical, qu'est-ce que c'est ?

Les objets connectés de santé sont classés dans la catégorie des ***dispositifs médicaux*** *pour l'ANSM et la CNIL. Adrien Rousseaux, expert en protection des données à caractère privé à la CNIL, apporte des éléments permettant de mieux comprendre les enjeux de la certification.*
Selon l'ANSM*, est considéré comme* ***dispositif médical*** *« tout instrument, appareil, équipement, logiciel, matière ou autre article, utilisé seul ou en association, y compris le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostique et/ou thérapeutique, et nécessaire au bon fonctionnement de celui-ci. Le dispositif médical est destiné par le fabricant à être utilisé chez l'homme à des fins de diagnostic, prévention, contrôle, traitement ou atténuation d'une maladie, d'une blessure ou d'un handicap ; mais aussi d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique. Son action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais sa fonction peut être assistée par de tels moyens » (directive européenne 93/42/CEE).*
Pour la CNIL*, c'est l'utilisation ou l'exploitation des données recueillies par les objets connectés de santé, ou de bien être, qui fait intervenir la loi Informatique et Libertés.*

Il n'y a pas de définition dans la loi française d'une donnée de santé permettant de la distinguer de la donnée de bien-être. Mais le ***règlement européen relatif à la protection des données personnelles****, adopté le 14 avril dernier, et qui sera applicable en 2018, apporte une définition légale qui toutefois n'est pas opposable (ne peut être utilisée comme argument juridique) mais le sera d'ici son application.* ***L'article 4 de ce règlement européen définit les données de santé*** *comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris les prestations de services, de soins de santé qui révèlent des informations sur l'état de santé de cette personne. »*
Des objets connectés de santé sont déjà commercialisés en tant que dispositifs médicaux :
Le Tensiomètre Bluetooth de Withings *se connecte aux smartphones et mesure la pression systolique, diastolique ainsi que le rythme cardiaque. Cet appareil a obtenu la certification européenne CE, il est donc certifié comme dispositif médical.*
L'électro-stimulateur connecté MyTens *de BewellConnect développé avec le laboratoire Visiomed se connecte aux smartphones et stimule des zones précises du corps avec des électrodes pour réduire les douleurs. Il est remboursé par la sécurité sociale, donc reconnu comme dispositif médical.*
MyECG, l'électrocardiogramme connecté *de BewellConnect développé avec le laboratoire Visiomed se connecte au smartphone et mesure la fréquence cardiaque. Il a reçu le marquage CE, ce qui en fait également un dispositif médical certifié.*

Tensiomètre sans fil de Withings, MyTens et MyECG de BewellConnect (Visiomed)

Quelles étapes pour certifier un objet de santé, dispositif médical ?

Afin de certifier un objet connecté comme dispositif médical, le fabricant doit d'abord constituer un dossier auprès d'un ***organisme notifié****. Ce dernier évalue la conformité aux exigences essentielles et délivre le certificat européen de marquage CE.*
La donnée de santé cible un risque de maladie. Les données issues d'un dispositif médical certifié peuvent être utilisées par un professionnel de santé. Les formalités auprès de la CNIL ne sont pas les mêmes pour un traitement de données de bien-être et un traitement de données de santé. En effet, les données de santé sont dites "sensibles" d'après l'article 8 de la loi Informatique et Libertés. Pour un objet connecté de bien-être, ne comportant donc pas de données de santé ou pour lequel le consentement de l'utilisateur est demandé, ***les formalités sont déclaratives****. Même si le traitement des données doit respecter la loi Informatique et Libertés (notamment le respect des droits des personnes à pouvoir s'opposer, à pouvoir rectifier ou tout simplement à pouvoir être informé et la mise en place de mesures de sécurité adaptées), l'entreprise doit simplement signaler les modalités d'usage à la CNIL. Pour les objets connectés de santé, ou de bien-être utilisant des données de santé, les* ***formalités nécessitent une autorisation de la CNIL*** *avant de pouvoir proposer le service délivré par l'objet connecté. En moyenne, les procédures prennent de 2 à 6 mois selon la disponibilité du responsable de traitement. Ce dernier est la personne ou l'entité qui définit le service proposé par un dispositif médical, et donc qui gère la transmission de données générées par ce dispositif médical à un serveur, le stockage des données, etc. Un certain nombre d'informations sont à fournir à l'usager d'après* ***l'article 32 de la loi informatique et libertés****. « La personne auprès de laquelle sont recueillies les données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le* ***responsable de traitement*** *ou son représentant :*
• De l'identité du responsable de traitement (qui va effectuer les traitements sur les données)
• Des finalités poursuivies par le traitement
• Du caractère obligatoire ou facultatif des réponses
• Des conséquences éventuelles d'un défaut de réponses (par exemple le service ne pourra pas être rendu dans son intégralité)
• Des destinataires ou catégories de destinataires des données
• Des droits de l'utilisateur sur ces données »
Le site de la CNIL propose un ***générateur de mentions "informatique et libertés"*** *équivalent aux mentions légales.*

Les intérêts de la certification pour l'utilisateur et le distributeur

Toutes ces démarches visent à protéger l'utilisateur de tout mésusage des dispositifs médicaux. C'est cette « digitalovigilance » qui garantit une communication maîtrisée des données de santé aux personnes souhaitées. L'usager ayant enregistré des données doit avoir connaissance des destinataires s'il y a transmission et il doit pouvoir maîtriser à qui il envoie quelles données.
*Sur de nombreux appareils, le système d'****API (Application Programming Interface = interface pour l'accès programmé aux applications)*** *permet à l'utilisateur de partager la donnée qui a été générée par un capteur avec un nouveau service, une application. Il peut à tout moment déconnecter les applications pour que les données cessent d'être transmises.*
*De nombreuses données transmises par les dispositifs médicaux peuvent être très utiles, dans le cadre de la recherche notamment. L'intérêt majeur de la certification des données de santé est donc qu'****elles peuvent être utilisées par des professionnels de santé****. De plus, un objet certifié dispositif médical peut être vendu en pharmacie : il peut être prescrit par un professionnel de santé et donc potentiellement pris en charge par la sécurité sociale.*

Bluetens et Beta-bioled : deux objets connectés vers la certification

Électrostimulateur connecté Bluetens / Test sanguin portable connecté Beta-Bioled

La société ***Bluetens*** *a développé un* ***électrostimulateur connecté*** *pour* ***soulager la douleur et se relaxer****. Son objectif premier est de créer un objet de santé qui se définit par sa fonction et son utilité. Il doit apporter plus que de l'analyse ou de la collecte de données. L'objectif est un réel changement d'état de l'utilisateur, l'objet doit avoir un impact remarquable sur la santé. L'électrostimulateur Bluetens est certifié ISO 13485 par une société de certification qui effectue un audit d'une part auprès de l'entreprise Bluetens, et d'autre part sur l'objet connecté de santé. Dans ce cas, c'est l'entreprise allemande TÜV agréée par les autorités européennes qui a certifié l'objet. L'ISO 13485 atteste que l'entreprise Bluetens respecte bien les normes nécessaires à l'élaboration de dispositifs médicaux. Cet appareil est donc certifié d'utilité médicale. Le but de l'entreprise étant de le distribuer le plus largement possible, il est vendu dans les enseignes de grande distribution spécialisées telles que Darty ou la Fnac.*
De son côté, la société ***Archimej Technology*** *est en train de développer* ***Beta-Bioled****,* ***un test sanguin portable et connecté****. Cette entreprise cherche à insérer sur le marché des dispositifs médicaux en franchissant toutes les étapes de la certification jusqu'à obtenir les agréments de la sécurité sociale pour que l'appareil puisse être remboursé. Cette démarche s'inscrit dans une volonté d'asseoir la crédibilité de Beta-Bioled face aux utilisateurs et au corps médical. Le processus de certification passe ici par 3 étapes dont la première est la formation auprès d'organismes spécialisés. Le biocluster Genopole leur apporte les conseils sur les questions des biotechnologies et Medicen facilite l'insertion d'innovations dans le domaine de la santé humaine vers les marchés industriels. La seconde étape, une fois l'objet conceptualisé et réalisé, consiste à réaliser des essais cliniques avec quelques milliers de tests dans des structures médicales. Enfin, l'objet sera certifié uniquement lorsque la Haute Autorité de Santé (HAS) aura validé toute la procédure. Et pour assurer une diffusion optimale dans le parcours médical, Archimej Technology souhaite obtenir l'agrément LPPR (Liste des Produits et Prestations Remboursables), qui permettra un remboursement de Beta-Bioled par l'Assurance Maladie. Ce parcours du combattant assurant une crédibilité et une valeur médicale peut prendre plusieurs années : l'objectif de mise sur le marché est fixé à 2018. En premier lieu, il sera distribué aux professionnels de santé (urgences, SAMU, maisons de retraite…). Ensuite la vente sera ouverte au grand public pour les malades chroniques, invalides légers ou séniors ne pouvant se déplacer en laboratoires. A terme l'objectif est de cibler les pharmacies comme canaux de distribution.*

Article original de Charles Deyrieux

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Certification des objets connectés de santé – Web des Objets

---

Ma vie disséquée à travers mes données personnelles

	Ma vie disséquée à travers mes données personnelles

---

Original de l’article mis en page : Ma vie disséquée à travers mes données personnelles

---

La Cnil épingle Windows 10 sur la collecte des données personnelles

La Cnil épingle Windows 10 sur la collecte des données personnelles

---

Constatant plusieurs manquements dont la collecte de données excessives et non pertinentes par Windows 10, la Cnil a mis en demeure Microsoft de se conformer à la loi dans un délai de 3 mois.

A quelques jours de la fin de la gratuité pour migrer sur Windows 10, la Cnil s'invite dans le débat sur le dernier OS de Microsoft. Et le moins que l'on puisse dire est que le régulateur n'est pas content des méthodes de l'éditeur américain. Elle vient de mettre en demeure Microsoft de se conformer dans un délai de 3 mois à la Loi Informatique et Libertés.

Alertée sur la collecte de données de Windows 10 (dont nous nous étions fait l'écho à plusieurs reprises : « pourquoi Windows 10 est une porte ouverte sur vos données personnelles » ou « Windows 10 même muet il parle encore »), la Cnil a effectué une série de contrôles entre avril et juin 2016 pour vérifier la conformité de Windows 10 à la loi.

De ces contrôles, il ressort plusieurs manquements. Le premier concerne une collecte des données excessives et non pertinentes. Elle reproche par exemple à Microsoft de connaître quelles sont les applications téléchargées et installées par un utilisateur et le temps passé par l'utilisateur sur chacune d'elles. Microsoft s'est toujours défendu de collecter des données personnelles en mettant en avant des relevés de « télémétrie » pour améliorer son produit.

Défaut de sécurité, absence de consentements et référence au Safe Harbor

Autre point soulevé par le régulateur, un défaut de sécurité a été trouvé dans le code PIN à 4 chiffres. Ce dernier est utilisé pour s'authentifier sur l'ensemble des services en ligne. Or le nombre de tentatives de saisie du code PIN n'est pas limité.

De plus, la Cnil constate une absence de consentement des personnes notamment sur le ciblage publicitaire lors de l'installation de Windows 10. Idem pour le dépôt de cookies déposés sur les terminaux des utilisateurs.

Enfin, cerise sur le gâteau, Microsoft est enjoint par la Cnil d'arrêter de se baser sur le Safe Harbor pour transférer les données personnelles aux Etats-Unis. Cet accord a été invalidé par la Cour de Justice de l'Union européenne en octobre 2015. Il a été remplacé par le Privacy Shield qui doit bientôt rentrer en vigueur.

La balle est maintenant dans le camps de Microsoft.

Article original de Jacques Cheminat

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : La Cnil épingle Windows 10 sur la collecte des données

Directive européenne sur la sécurité des réseaux et des systèmes d’information

	Directive européenne sur la sécurité des réseaux et des systèmes d’information

Les entreprises qui fournissent des services essentiels, par exemple l'énergie, les transports, les services bancaires et de santé, ou numériques, tels que les moteurs de recherche et les services d'informatique en nuage, devront améliorer leur capacité à résister à des cyber-attaques, selon les premières règles de cybersécurité à l'échelle européenne, approuvées par les députés mercredi.

L'établissement de normes de cybersécurité communes et renforcer la coopération entre les pays de l'Union aidera les entreprises à se protéger elles-mêmes, et aussi à prévenir les attaques contre les infrastructures interconnectées des pays européens, estiment les députés.

« Des incidents de cybersécurité possède très souvent un aspect transfrontalier et concernent donc plus d'un État membre de l'Union européenne. Une protection fragmentaire de la cybersécurité nous rend tous vulnérables et pose un risque de sécurité important pour l'Europe dans son ensemble. Cette directive établira un niveau commun de sécurité de réseau et d'information et renforcera la coopération entre les États membres. Cela contribuera à prévenir à l'avenir les cyberattaques sur les infrastructures interconnectées européennes importantes », a déclaré le rapporteur du Parlement Andreas Schwab (PPE, DE).

La directive européenne sur la sécurité des réseaux et des systèmes d'information « est également l'un des premiers cadres législatifs qui s'applique aux plates-formes. En phase avec la stratégie du marché unique numérique, elle établit des exigences harmonisées pour les plates-formes et veille à ce qu'elles puissent observer des règles similaires quel que soit l'endroit de l'Union européenne où elles opèrent. C'est un énorme succès et une première étape importante vers l'établissement d'un cadre réglementaire global pour les plates-formes dans l'Union », a-t-il ajouté.

Les pays de l'UE devront lister les entreprises de « services essentiels »

La nouvelle législation européenne prévoit des obligations en matière de sécurité et de suivi pour les « opérateurs de services essentiels » dans des secteurs tels que ceux de l'énergie, des transports, de la santé, des services bancaires et d'approvisionnement en eau potable. Les États membres de l'UE devront identifier les entités dans ces domaines en utilisant des critères spécifiques, par exemple si le service est essentiel pour la société et l'économie, et si un incident aurait des effets perturbateurs considérables sur la prestation de ce service.

Certains fournisseurs de services numériques – les marchés en ligne, les moteurs de recherche et les services d'informatique en nuage – devront aussi prendre des mesures pour assurer la sécurité de leur infrastructure et devront signaler les incidents majeurs aux autorités nationales. Les exigences de sécurité et de notification sont, cependant, plus légères pour ces fournisseurs. Les micro- et petites entreprises numériques seront exemptées de ces exigences.

Mécanismes de coopération à l'échelle européenne

Les nouvelles règles prévoient un « groupe de coopération » stratégique pour échanger l'information et aider les États membres à renforcer leurs capacités en matière de cybersécurité. Chaque pays de l'Union devra adopter une stratégie nationale relative à sécurité des réseaux et des systèmes d'information.

Les États membres devront aussi mettre en place un centre de réponse aux incidents de sécurité informatique (CSIRT) pour gérer incidents et risques, discuter des questions de sécurité transfrontalière et identifier des réponses coordonnées. L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) jouera un rôle clé dans la mise en œuvre de la directive, en particulier en matière de coopération. La nécessité de respecter les règles de protection des données est réitérée tout au long de la directive.

Prochaines étapes

La directive sur la sécurité des réseaux et des systèmes d'information sera bientôt publiée au Journal officiel de l'Union européenne et entrera en vigueur le vingtième jour suivant sa publication. Les États membres auront alors 21 mois pour transposer la directive dans leur législation nationale et six mois supplémentaires pour identifier les opérateurs de services essentiels.

Directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Procédure: codécision, seconde lecture
Source : Parlement européen

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybersécurité: les députés soutiennent les règles pour aider les entreprises de services clés à… – Linkis.com

---

L’Internet russe prêt à ériger des frontières

L’Internet russe prêt à ériger des frontières

La Russie prévoit de contrôler davantage la partie russe du réseau Internet et son trafic, y compris l'activité des serveurs DNS et l'attribution des adresses IP.

L'an dernier, la Russie a annoncé l'entrée en vigueur d'une loi obligeant toute organisation détenant des données de citoyens russes à les stocker sur des serveurs se trouvant physiquement sur le territoire russe. Cette année, un autre projet de loi concocté par le ministère russe des communications, prévoit la création d'un système de surveillance du trafic Internet, y compris l'activité des serveurs DNS (système de noms de domaine) et l'attribution des adresses IP.
Le texte, dont le journal *Vedomosti* s'est fait l'écho, vise à réguler *« la partie russe du réseau Internet »*. Et ce officiellement pour renforcer la protection de l'Internet russe face aux cyberattaques. Le projet implique aussi la surveillance du trafic Internet transfrontalier, en s'appuyant notamment sur le système SORM (système pour activité d'enquête opératoire). Reste à savoir si la Russie a les moyens de faire appliquer de telles restrictions, dont elle devra mesurer l'impact économique.

Réseau de réseaux

Dave Allen, vice-président et avocat général de Dyn, un spécialiste de la performance réseau basé dans le New Hampshire, aux États-Unis, a publié une tribune sur le sujet dans *Venturebeat*. Allen observe qu'une grande partie du trafic Internet russe dépend actuellement beaucoup de pays avec lesquels la Russie entretient des relations compliquées, voire conflictuelles.
Les données partagées de Moscou à Saint-Pétersbourg par un abonné de l'opérateur mobile russe MegaFon, par exemple, transitent 9 fois sur 10 par Kiev, en Ukraine, selon lui. Et plus de 40 % des données qui passent par le réseau de MTS, le premier opérateur mobile russe, pour aller aussi à Saint-Pétersbourg, transiteraient par Amsterdam aux Pays-Bas et par Francfort en Allemagne.
La tendance se vérifie auprès d'entreprises publiques : ainsi, plus de 85 % des données transmises de Moscou vers Saint-Pétersbourg par TransTelekom, filiale de la Compagnie des chemins de fer russes, passeraient par Francfort. Et la plupart des données qui quittent la Russie, selon Dave Allen, passent par le backbone RETN, qui a des points de présence en Europe centrale et orientale.

Localisation de données

Les mesures de renforcement de la protection des données russes s'appliquent à toutes les entreprises ayant une activité dans le pays. L'an dernier, le régulateur russe Roskomnadzor a mené un audit auprès de 317 sociétés et administrations. Il a estimé que 2 étaient dans l'illégalité. L'audit pourrait être étendu cette année à d'autres grands groupes, dont Microsoft, HPE et Citibank.
Pour que les données puissent être transférées temporairement à l'étranger, une protection *« adéquate »* de ces données doit exister. L'Ukraine, l'Allemagne et les Pays-Bas ont signé une convention sur le traitement automatisé de données personnelles qui semble satisfaire cette condition. En revanche, le doute persiste sur le chiffrement. Le gouvernement russe, comme d'autres, envisage de l'affaiblir pour donner plus de marge de manoeuvre à ses services de renseignement.
D'autres pays ont fait des propositions en faveur de la localisation de données. En France, un amendement qui prévoyait l'interdiction de traitement de données personnelles stockées hors d'un État membre de l'Union européenne, a finalement été écarté du projet de loi République numérique.
Article original de Ariane Beky

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : L'Internet russe prêt à

ériger des frontières