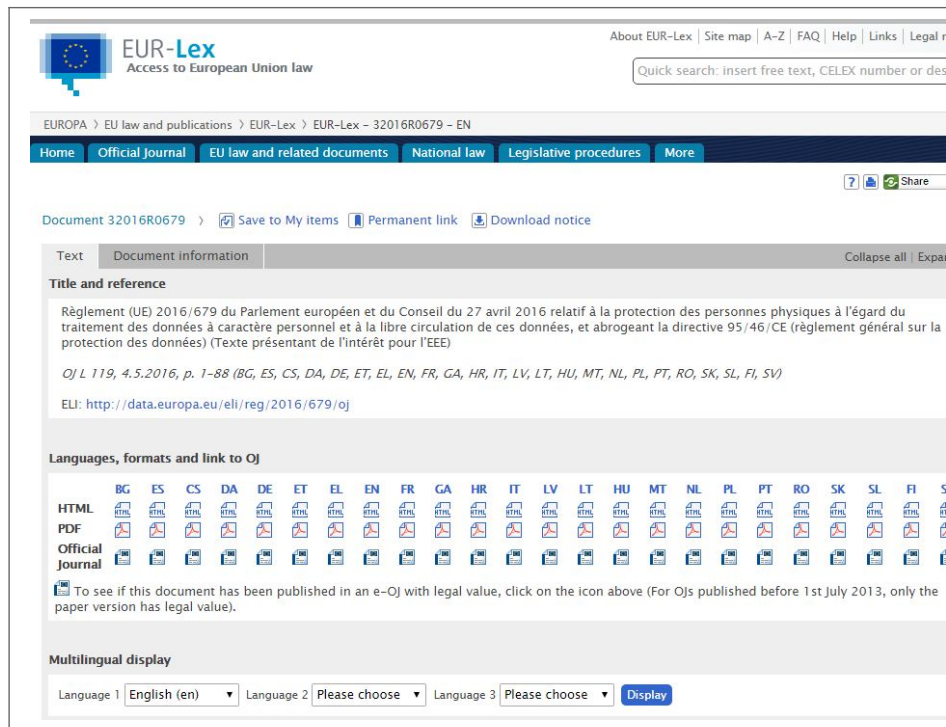


Introduction au Règlement Européen sur la Protection des Données



The screenshot displays the EUR-Lex website interface. At the top, the EUR-Lex logo and navigation links are visible. The main content area shows the document 32016R0679, which is the General Data Protection Regulation (GDPR). The document is in French, titled "Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)". The document is available in multiple languages, as indicated by the "Languages, formats and link to OJ" section. The "Multilingual display" section at the bottom allows users to view the document in different languages, with "English (en)" selected for Language 1.

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 meilleures 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.



[Contactez-nous](#)



Réagissez à cet article

CNIL : nouvelle norme simplifiée pour la scolarité des mineurs

	<p>CNIL nouvelle norme simplifiée pour la scolarité des mineurs</p>
--	---

Dans le cadre de son programme de simplification des formalités préalables pour les collectivités territoriales, la Cnil a adopté une norme simplifiée unique qui met à jour et abroge le cadre existant.

Le 10 décembre 2015, la Commission a adopté une norme simplifiée n°NS-058 qui fusionne et abroge les normes simplifiées n°NS-027 et n°NS-033. En effet, ces normes étaient désuètes et ne répondaient pas aux nouvelles préoccupations des acteurs concernés. Elle a été présentée sur le site de la Cnil le 12 août dernier.

Cette nouvelle norme permet de simplifier, pour ces traitements courants, les démarches des collectivités territoriales et des organismes en charge d'un service scolaire, périscolaire et de petite enfance. Elle offre un cadre unifié et adapté aux contraintes liées à la gestion de ces services.

Après avoir vérifié que leur traitement s'inscrit précisément dans le champ d'application de cette norme, les responsables de traitements de données concernés devront effectuer un engagement de conformité à la norme NS-058 auprès de la CNIL.

Les personnes concernées

Cette norme s'adresse aux collectivités territoriales, aux personnes morales de droit public et aux personnes morales de droit privé gérant un service public...[lire la suite]

En savoir plus

Le communiqué de la Cnil du 12 août dernier avec une présentation synthétique de la norme :

<https://www.cnil.fr/fr/une-nouvelle-norme-simplifiee-ns-058-pour-la-gestion-des-affaires-scolaires-periscolaires>

Le résumé succinct de la norme :

<https://www.cnil.fr/fr/declaration/ns-058-affaires-scolaires-periscolaires-extrascolaires-et-petite-enfance>

La norme NS-058 elle-même sur *Légifrance* :

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032788919>

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.




[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Données personnelles : nouvelle norme simplifiée pour la scolarité des mineurs

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

<p>Denis JACOPINI</p>  <p>vous informe</p>	<p>Protection des données personnelles, plus que quelques mois pour se mettre en règle...</p>
---	---

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 reprises 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 fait 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 personnelles 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 conformité.

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.



[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.



[Contactez-nous](#)

Réagissez à cet article

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

Collectes massives et illégales par le Renseignement allemand

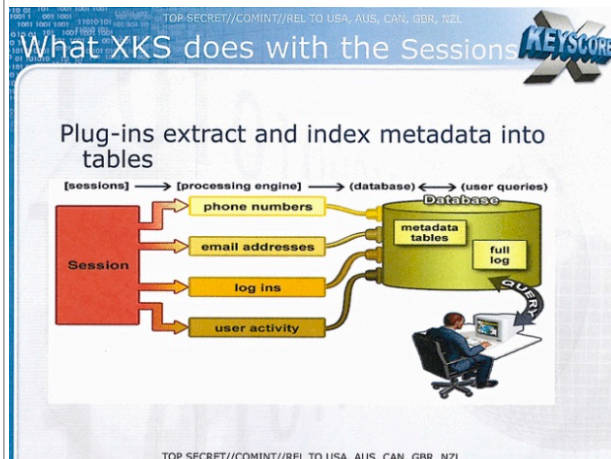


Collectes
massives et
illégales par
le
Renseignement
allemand

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine. Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.

L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.



Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête...[lire la suite]

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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama

Retrouver l'auteur d'un E-mail à partir de l'adresse IP : Le demandeur condamné



Retrouver
l'auteur
d'un E-
mail à
partir de
l'adresse
IP : Le
demandeur
condamné

Le TGI de Meaux a débouté l'entreprise qui voulait obtenir de Numericable les noms, prénoms, adresses et coordonnées complètes de l'auteur d'un email frauduleux à partir de son adresse IP.

Dans une ordonnance de référé du 10 août 2016 repérée par Legalis, le tribunal de grande instance de Meaux (Seine-et-Marne) a débouté l'entreprise qui voulait obtenir de Numericable les données d'identification correspondant à l'adresse IP de l'auteur présumé d'un email frauduleux.

Comment en est-on arrivé là ? En début d'année, la société France Sécurité a préparé une proposition commerciale à l'attention d'Airbus Helicopters dans le cadre d'un appel d'offres. Dans la foulée, le distributeur d'équipements de protection individuelle a reçu un courriel d'un individu se faisant passer pour un employé d'Airbus et lui demandant de transmettre par courriel le fichier contenant la proposition... Suspectant la fraude, France Sécurité a contacté Airbus. Le nom associé au courriel était bien celui d'un de ses employés, mais il n'était pas l'auteur des courriels en question.

Usurpation d'identité

Dans un premier temps, une plainte a été déposée contre X pour usurpation d'identité. Parallèlement, le département informatique de France Sécurité a identifié l'adresse IP de l'expéditeur du courriel (transmis via Gmail) ainsi que le FAI hôte, à savoir : Numericable. Un procès-verbal de constat d'huissier a été établi. Ensuite, le 28 juin 2016, France Sécurité a déposé plainte auprès du procureur de la République près le tribunal de grande instance de Nantes. Et le 8 juillet 2016, l'entreprise a fait assigner devant le juge des référés du TGI de Meaux le câblo-opérateur. Le but : obtenir du tribunal qu'il ordonne au FAI de communiquer dans un délai de 48 heures les données d'identification correspondant à l'adresse IP en cause. Car, selon le demandeur, le câblo-opérateur est tenu de conserver les données permettant l'identification de son client et de déférer aux demandes de l'autorité judiciaire. Et ce en application de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004. France Sécurité souhaitait également qu'une astreinte soit versée par Numericable en cas de dépassement de ce délai, en plus des frais irrépétibles... Sans succès.

L'adresse IP, une donnée personnelle

Le juge est parti du principe que l'adresse IP est une donnée à caractère personnel. Par ailleurs, il a considéré que la collecte de cette donnée constitue un traitement au sens de la loi informatique et libertés. Une telle collecte aurait donc dû faire l'objet d'une autorisation de la Commission nationale informatique et libertés (Cnil) accordée à France Sécurité. Cela n'a pas été le cas. Par ailleurs, le juge considère que le cadre juridique applicable dans ce dossier ne peut pas être celui de la LCEN de 2004. Selon lui, Numericable n'est pas visé en tant que « personne dont l'activité est d'offrir un accès à des services de communication au public » en relation avec « la création d'un contenu » en ligne.

Résultat : le TGI de Meaux a débouté France Sécurité de toutes ses demandes. L'entreprise a été condamnée aux entiers dépens et au versement de 2 000 euros au titre des frais irrépétibles...[lire la suite]

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.



[Contactez-nous](#)

Réagissez à cet article

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 réinventé, 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 prêts 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, conteneurs, 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.



Contacter-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

Privacy Shield adopté,

nouveau fondement pour les transferts de données outre-atlantique



Privacy Shield
adopté, nouveau
fondement pour
les transferts
de données
outre-atlantique

L'adoption de ce nouveau « bouclier de protection des données personnelles » est le fruit d'un long processus, commencé dès 2014, avec la révélation par l'ancien agent de la CIA Edward Snowden de la surveillance de masse effectuée par les services de renseignements américains puis par le refus, sur ce motif, d'un citoyen américain de transférer ses données vers les États-Unis. Le Cour de Justice de l'Union Européenne a ainsi dans une décision du 6 octobre 2015 déclaré invalide la décision de la Commission du 26 juillet 2000 constatant que les États-Unis assurent un niveau de protection adéquat aux données caractères personnel transférées. En effet la Cour a considéré que les États-Unis « n'apportent pas les garanties suffisantes pour protéger les données des citoyens européens au motif que les pouvoirs des services de renseignements américains s'étendent à toutes données exportées depuis l'Europe dès lors que l'intérêt de sécurité publique est en cause ». La Commission a alors proposé une série de mesures destinées à améliorer la protection des données des citoyens européens. A la suite de cette décision, l'ensemble des transferts de données personnelles vers des entités situées aux États-Unis sur le fondement du Safe Harbor ont été interrompus et des solutions alternatives mises en place. Le Groupe de travail de l'Article 29, qui est constitué des différents autorités de protection des données de l'Union européenne, a élaboré une série de recommandations destinées à améliorer la protection des données, telles que les clauses contractuelles types et les règles d'entreprise contraignantes (RCR).

En parallèle la Commission européenne et le gouvernement américain engageant des discussions afin de trouver un nouvel accord sur le transfert des données personnelles des citoyens européens vers les États-Unis. Le 28 février 2016, la Commission européenne a présenté un projet d'accord politique. La Commission a présenté le projet d'accord le 28 février 2016. Le groupe de travail « Article 29 » a ensuite rendu un premier avis le 13 avril 2016 après critique en particulier sur l'insuffisance des garanties pour les citoyens européens pour contrôler l'usage de leurs données.

Une résolution a été adoptée le 26 mai par le Parlement européen, et la Commission a clôturé la procédure d'adoption du nouvel accord le 12 juillet 2016 en adoptant une décision d'adéquation visant à reconnaître au mécanisme « EU-U.S. Privacy Shield » un niveau de protection « essentiellement équivalent » aux exigences

Le Privacy Shield vise à permettre aux entreprises de transférer plus facilement vers les Etats Unis des données personnelles collectées dans l'Union européenne, tout en protégeant les droits des personnes concernées.

Des obligations strictes pour les entreprises qui traitent des données : dans le cadre du nouveau dispositif, le ministère américain du commerce procèdera régulièrement à des mises à jour et à des réexamens concernant les entreprises participantes, afin de veiller à ce qu'elles observent les règles auxquelles elles ont souscrit. Les entreprises dont la pratique ne sera pas conforme aux nouvelles règles s'exposent à des sanctions et à une radiation de la liste des entreprises adhérentes au dispositif.

Un accès plus sûr aux données : les citoyens américains pourront accéder plus facilement à leurs données personnelles détenues par les services publics fédéraux, les États ou les collectivités locales. Des fins d'ordre public et de sécurité nationale seront soustraites aux données soumises aux conditions de transparence. Les données relatives à la santé, à l'éducation, à la justice, à la sécurité nationale et à la défense resteront protégées. Les mécanismes de surveillance bien définis. De même, tous les citoyens d'un État bénéficiant pour la première fois de mécanismes de recours dans ce domaine. Les États-Unis ont exclu toute surveillance de masse systématique des données à caractère personnel transférées vers leur territoire dans le cadre du protection des données UE-États-Unis. Le secrétaire d'État américain a instauré une possibilité de recours pour les Européens dans le domaine du renseignement national en créant un mécanisme de médiation au sein du département d'État ;

Une coopération renforcée entre autorités américaines et européennes : le règlement des litiges transatlantiques sera régi par l'un ou l'autre des deux systèmes existants de règlement des différends. Les citoyens européens auront également accès à un mécanisme d'arbitrage sans précédent, en dernier ressort. La possibilité d'un recours dans le domaine de la sécurité nationale ouverte aux citoyens de l'UE passera par un médiateur indépendant des services de renseignement des États-Unis ;

Le respect des principes de confidentialité et de sécurité nationale : le recensement sera soumis à la Commission européenne et le Ministère américain du Commerce, lesquels y associeront des experts nationaux du renseignement travaillant au sein des autorités américaines et européennes de protection des données. La Commission s'appuiera sur toutes les autres sources d'information disponibles et adressera un rapport annuel au Parlement européen et au Conseil,

Un accord déjà critiqué

Le G29 dans son avis d'avril 2016 avait notamment fait part de ses préoccupations sur certains nombre de points nanquents, incomplets ou peu clairs. Le G29 avait en particulier regretté l'absence de plusieurs principes tels que la limitation de la durée de conservation et l'interdiction des décisions automatisées. En ce qui concerne l'accès par les autorités publiques aux données, le G29 avait déploré que les autorités américaines n'aient pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens. Enfin, le G29 avait eu des doutes sur l'indépendance du médiateur (ombudsperson) et sur le fait qu'il dispose de pouvoirs suffisants pour exercer son rôle efficacement et permettre d'obtenir un recours satisfaisant en cas de désaccord avec l'administration.

Il n'est pas certain que la nouvelle rédaction satisfasse pleinement le G29.

Article original de DLA PIPER



Original de l'article mis en page : Adoption du Privacy Shield par la Commission européenne : un nouveau fondement pour les transferts de données outre-atlantique, Partenaire – Les Echos Business

Certification des objets connectés de santé – Web des Objets



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'intègrent 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



Electrostimulateur 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 de 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 seniors ne pouvant se déplacer en laboratoire. 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 téléphoniques, 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

Ma vie disséquée à travers mes données personnelles

