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

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

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

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

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

II- Principales mesures du RGPD

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

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

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

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

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

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

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

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

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

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

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

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

Vigilance – faux appels passés au nom de la CNIL

Vigilance – faux appels passés au nom de la CNIL

Vigilance – faux appels passés au nom de la CNIL

Des entreprises ont reçu, ces derniers jours, des appels téléphoniques de personnes se faisant passer pour la CNIL et prétextant devoir envoyer des documents.
Ces appels frauduleux ont pour but de collecter des informations sur votre organisation, et notamment l'adresse mail de dirigeants (directeur informatique, directeur des achats, etc.), pour préparer une attaque informatique (rançongiciel / ransomware) ou une escroquerie financière (« arnaque au Président »).
N'y répondez pas ! En cas de doute, vous pouvez contacter la CNIL au 01 53 73 22 22

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Vigilance – faux appels passés au nom de la CNIL | CNIL

Demande dannulation du Privacy Shield par UFC-Que Choisir

Demande d'annulation du Privacy Shield par UFC Que Choisir

Alors que la protection des données personnelles est une préoccupation majeure des consommateurs, l'UFC-Que Choisir, compte tenu des risques que fait peser l'accord transatlantique sur la protection des données personnelles (Privacy Shield), intervient en soutien de deux recours en annulation contre cet accord.

Après l'invalidation en 2015 par la Cour de justice de l'Union européenne de l'accord encadrant le transfert de données entre les Etats-Unis et l'Europe, le « Safe Harbour », compte tenu du niveau de protection insuffisant des consommateurs européens, l'Union européenne a négocié un nouvel accord avec les Etats-Unis, le Privacy Shield. Cet accord a été adopté le 8 juillet 2016, malgré les inquiétudes formulées par le Parlement européen, plusieurs gouvernements, les CNIL et les associations de consommateurs européennes.

Loin de renforcer significativement le cadre juridique du transfert des données personnelles aux Etats-Unis et d'offrir un niveau de protection « adéquate », comme exigé par les textes communautaires, le nouvel accord n'offre qu'une protection lacunaire aux ressortissants européens :

L'admission d'une collecte massive et indifférenciée des données personnelles par les services de renseignements américains

Les lois américaines autorisent encore aujourd'hui, malgré les critiques formulées dans le cadre de l'invalidation du Safe Harbour, la collecte massive d'information par la NSA et les services de renseignement américains auprès des entreprises détentrices de données personnelles, incluant des données de consommateurs français qui ont été transférées aux Etats unis.

Bien que le gouvernement américain se soit moralement engagé à réduire cette collecte autant que possible, aucune mesure concrète n'a encore été mise en place pour limiter ces traitements de données personnelles.

Cette situation est d'autant plus inquiétante que les autorités américaines sont aussi autorisées, sur la seule base de vos données personnelles, à rendre des décisions susceptibles de produire des effets juridiques préjudiciables à votre égard. Ainsi, suite à l'envoi d'un message privé sur Facebook, exprimant une opinion politique ou critiquant la collecte à tous crins des données par les multinationales américaines, vous pourriez vous voir interdire l'entrée aux Etats Unis par les autorités américaines !

Un ersatz de droit au recours pour les consommateurs européens

Alors que le droit européen exige un droit au recours effectif et un accès à un tribunal impartial, le dispositif de réclamation prévu par le Privacy Shield est stratifié et complexe… Le principal recours en cas de décision préjudiciable rendue par les autorités américaines à l'encontre d'un ressortissant européen, est un médiateur… nommé par le Secrétaire d'état américain.

Enfin, le droit de s'opposer à un traitement est prévu uniquement en cas de «modification substantielle de la finalité du traitement », alors même que le droit européen offre le droit de s'opposer à un traitement de ses données personnelles à tout moment, aussi bien lors de la collecte, qu'en cours de traitement de données personnelles.

Dans le contexte de mondialisation des échanges et de transfert des données vers des Etats avec des niveaux moindres de protection que le niveau européen, ces risques sont loin d'être théoriques comme l'a souligné récemment l'association s'agissant de la collecte de données via des jouets connectés ou des applications mobiles et leur transfert vers les Etats-Unis.

Au vu de ces éléments inquiétants, deux recours en annulation ont été déposés en septembre 2016 devant le Tribunal de l'Union européenne : l'un par le 'Digital Right Ireland', groupe lobbyiste Irlandais de défense de la vie privée sur Internet, l'autre par les 'Exégètes amateurs', groupe de travail regroupant trois associations françaises…[lire la suite]

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

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Protection des données personnelles : demande dannulation du Privacy Shield — UFC-Que Choisir

Les particuliers victime d’une attaque par Ransomwares toutes les 10 secondes

	Les particuliers victime d’une attaque par Ransomwares toutes les 10 secondes

Entre janvier et septembre 2016, le nombre d'attaques de ransomware contre les entreprises a triplé. En septembre, Kaspersky Lab enregistrait une attaque de ce type toutes les 40 secondes contre une toutes les 2 minutes en début d'année. Une entreprise sur cinq dans le monde est concernée.

Selon un rapport de l'entreprise de sécurité Kaspersky Lab, entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises est passée de deux minutes à 40 secondes. Pour le grand public, la situation est encore pire : en septembre, la fréquence des attaques est passée à 10 secondes. Au cours du troisième trimestre de l'année, Kaspersky Lab a détecté 32 091 nouvelles versions de ransomware contre seulement 2 900 au cours du premier trimestre. « Au total, nous avons comptabilisé 62 nouvelles familles de malwares de cette catégorie cette année », a indiqué l'entreprise de sécurité. Ce nombre montre aussi très clairement l'intérêt des cybercriminels pour ce type de malwares dont la réussite reste constante malgré les actions menées par les autorités policières et judiciaires et les outils de décryptage gratuits fournis par les chercheurs et les entreprises de sécurité.

L'enquête réalisée par Kaspersky Lab montre aussi que les petites et moyennes entreprises ont été les plus touchées : au cours des 12 derniers mois, 42 % d'entre elles ont été victimes d'une attaque par un ransomware. Parmi elles, une PME sur trois a payé la rançon, mais une sur cinq n'a jamais récupéré ses fichiers après le paiement. « Au total, 67 % des entreprises touchées par un ransomware ont perdu une partie ou la totalité de leurs données d'entreprise et une victime sur quatre a passé plusieurs semaines à essayer de retrouver l'accès à ses fichiers », ont déclaré les chercheurs de Kaspersky. Cette année, le ransomware le plus populaire est indéniablement CTB-Locker, utilisé dans 25 % des attaques. Viennent ensuite Locky, pour 7 % des attaques, et TeslaCrypt, pour 6,5 %, même si cette famille de ransomware a été active jusqu'en mai seulement. Les auteurs d'attaques par ransomware ont également affiné leurs cibles : leurs campagnes de phishing et d'ingénierie sociale visent des entreprises spécifiques ou des secteurs de l'industrie où le manque de disponibilité des données est très dommageable à leur activité…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Ransomware : une attaque toutes les 40 secondes contre les PME – Le Monde Informatique

---

Alerte : Des routeurs domestiques attaqués par malvertising via DNSChanger

Alerte : Des routeurs domestiques attaqués par malvertising via DNSChanger

---

Des routeurs domestiques font l'objet d'une attaque par le biais d'une campagne de publicités malveillantes et via le navigateur Web sur Windows et Android.

Depuis la fin du mois d'octobre, les chercheurs en sécurité de Proofpoint indiquent avoir constaté l'utilisation d'une version améliorée du kit d'exploits DNSChanger dans le cadre de campagnes de publicités malveillantes (du malvertising).
Pour ce retour, DNSChanger – qui avait infecté des millions d'ordinateurs en 2012 – cible des routeurs domestiques et fonctionne la plupart du temps via le navigateur Google Chrome sur Windows et les appareils Android. Toutefois, il s'agit bel et bien d'exploiter des vulnérabilités affectant des routeurs.
Du code JavaScript malveillant permet de révéler une adresse IP locale par le biais d'une requête WebRTC (Web Real-Time Communication) vers un serveur STUN (Session Traversal Utilities for NAT) de Mozilla. WebRTC est un protocole pour la communication en temps réel sur le Web, et STUN est un protocole permettant de découvrir l'adresse IP et le port d'un client ainsi que déterminer des restrictions au niveau du routeur.

Si l'adresse IP est jugée digne d'intérêt, une fausse publicité est affichée. Elle prend la forme d'une image au format PNG. Un code exploit est caché dans les métadonnées et pour rediriger la victime vers une page hôte de DNSChanger.

Proofpoint explique que DNSChanger va une nouvelle fois vérifier l'adresse IP locale de la victime grâce à des requêtes STUN. Puis, le navigateur Google Chrome chargera plusieurs fonctions et une clé de chiffrement AES cachée par stéganographie dans une petite image. La clé sert à dissimuler du trafic et décrypter une liste d'empreintes numériques afin de déterminer si un modèle de routeur est vulnérable.
L'attaque menée dépend du modèle de routeur. Elle est utilisée pour modifier les entrées DNS (Domain Name System ; correspondance entre un nom de domaine et une adresse IP) dans le routeur et tenter de rendre accessibles les ports d'administration depuis des adresses externes. Le chercheur Kafeine de Proofpoint évoque alors une exposition du routeur à d'autres attaques et cite l'exemple des botnets Mirai.
À noter que s'il n'y a pas d'exploits connus, une attaque tentera tout de même sa chance en essayant de tirer parti d'identifiants qui sont ceux par défaut (pas modifiés par l'utilisateur), et toujours pour modifier les paramètres DNS.
Soulignons bien que le navigateur n'est ici pas mis en cause…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : DNSChanger attaque des routeurs domestiques via malvertising

---

Victime de Ransomware ? Payer ou ne pas payer ?

Victime de Ransomware ? Payer ou ne pas payer ?

Selon une étude d'IBM, près de 70% des entreprises victimes d'un ransomware acceptent de payer les cybercriminels pour récupérer leurs données. 50% de celles-ci ont versé plus de 10.000 dollars. Pourquoi payer ? Pour récupérer l'accès à leurs données critiques.

« On ne paie pas, ce n'est pas une solution raisonnable » jugeait en début d'année le patron de l'agence de sécurité de l'Etat (Anssi). Pour Guillaume Poupard, verser des rançons aux auteurs de ransomware n'est pas la solution.

Pourquoi ? Car, entre autres, « cela contribue uniquement à soutenir financièrement les développeurs du malware » justifie Catalin Cosoi, responsable de la stratégie sécurité de BitDefender. Mais voilà, faute de sauvegarde et compte tenu de l'importance des données, des entreprises se résignent à payer.

Ransomware : des attaques à large spectre

C'est ce qu'observe IBM Security dans une étude. D'après Big Blue, les entreprises sont de plus en plus victimes de ransomware. Mais d'abord par opportunisme. Ces attaques sont désormais bien moins ciblées et affectent des victimes plus que des cibles.

L'attaque fin novembre contre le système de transport de San Francisco en est une illustration. Les pirates expliquaient ainsi automatiser l'infection par un ransomware après détection de vulnérabilités. La municipalité avait cependant refusé de payer la rançon de 100 bitcoins (alors plus de 70.000 dollars).

Selon IBM, la rentabilité du ransomware encourage à la multiplication des attaques. Près de 40% des emails de spam contiendraient désormais un tel programme malveillant. Cela se traduit mécaniquement par une hausse du nombre de victimes.

Et les entreprises victimes auraient donc majoritairement tendance, à près de 70%, à payer la rançon pour récupérer leurs données, chiffrées par les cybercriminels et donc inexploitables. Le préjudice financier dépasserait les 10.000 dollars pour 50% de ces sociétés.

Payer ou renoncer à ses données critiques

Les 20% restants auraient versé plus de 40.000 dollars, estime IBM. Au total, Big Bue évalue à 1 milliard de dollars, le montant ainsi extorqué aux entreprises grâce à un ransomware…[lire la suite]

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

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ransomware – Payer ou ne pas payer ? Une large majorité d'entreprises a choisi – ZDNet

---

Piratage de Yahoo : les données sont à vendre depuis août 2016

Désormais connu de tous, le piratage de la base de données des utilisateurs a commencé à apparaître à la lumière en août dernier, quand Andrew Komarov, le responsable du renseignement (sic) de la firme américaine InfoArmor a découvert qu'un collectif de hackers d'Europe de l'Est off…[Lire la suite]

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

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

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.

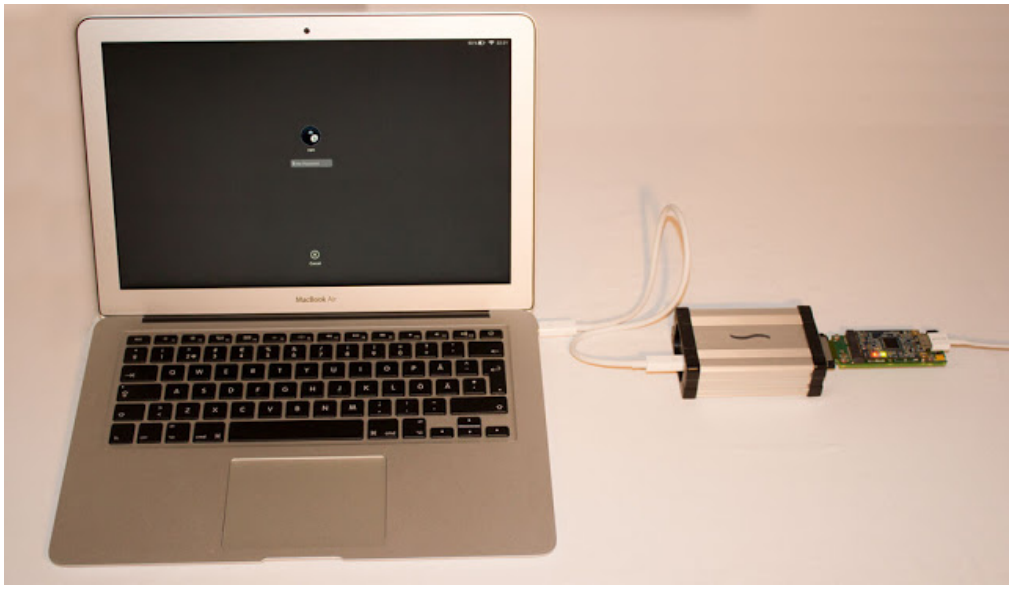
Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

---

300 dollars et 30 secondes pour pirater un Mac



300 dollars et 30 secondes pour pirater un Mac

Encore une méthode pour pirater un Mac en veille ou verrouillé. Un dispositif peut récupérer le mot de passe en quelques secondes.
Un expert en sécurité suédois, Ulf Frisk, a concocté une méthode pour voler le mot de passe d'un Mac en veille ou verrouillé. Pour cela, il utilise un dispositif qu'il branche sur le port Thunderbolt de l'appareil, en l'occurrence un MacBook Air. Mais cela pourrait marcher aussi sur un port USB de type C.
Prix de l'équipement en question : 300 dollars. Pour réaliser son exploit, il s'appuie sur une faille présente dans FileVault 2. Plus précisément, la brèche se situe dans la capacité donnée aux périphériques Thunderbolt d'accéder à mémoire directe (DMA) du Mac, avec des droits d'écriture et de lecture. Or dans cette zone, le mot de passe du disque chiffrée est stocké en clair, même lorsque l'ordinateur est verrouillé ou quand le système redémarre. Le mot de passe est placé dans plusieurs zones mémoires mais sur une plage fixe, donnant un moment de lisibilité pour un pirate. Ce laps de temps n'est que de quelques secondes au moment du redémarrage du système. Le dispositif d'Ulf Frisk profite de ce timing pour voler le mot de passe…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

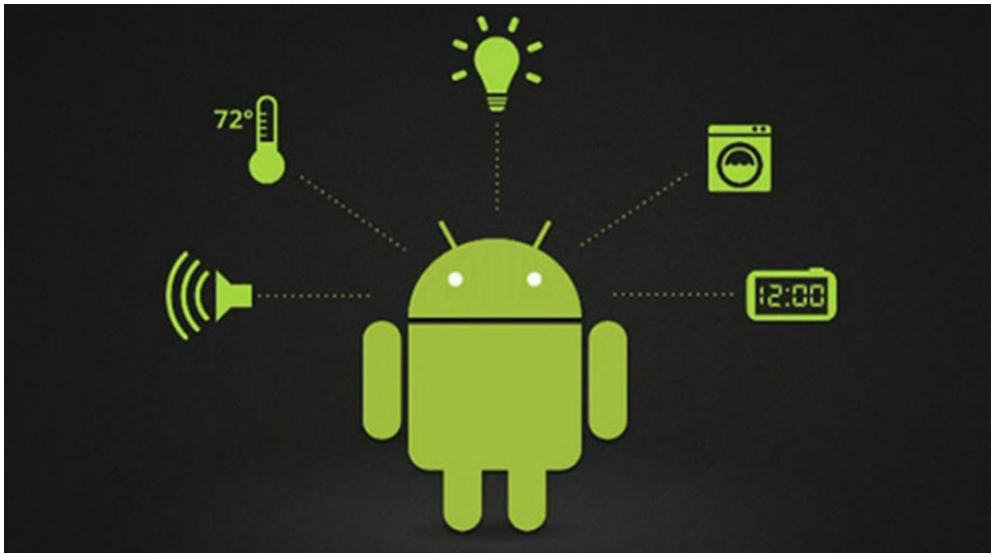
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

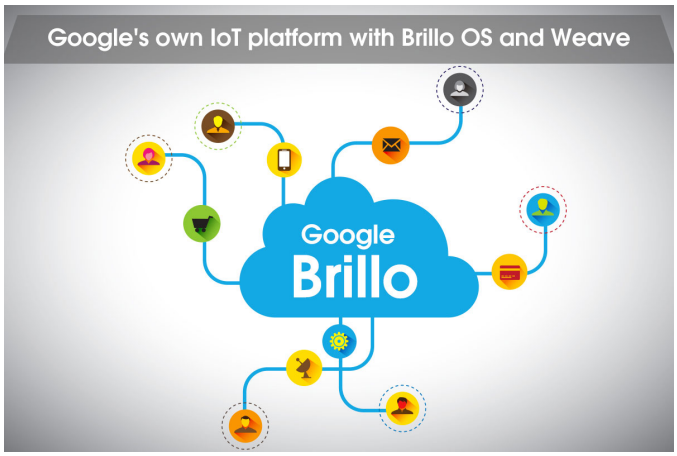
Original de l'article mis en page : Pirater un Mac en 30 secondes vous coûtera 300 dollars

Android Things , le nouvel OS pour objets connectés de Google



Android Things , le nouvel OS pour objets connectés de Google

En 2015, lors de sa conférence annuelle Google I/O, le géant de Mountain View dévoilait Brillo, un système d'exploitation destiné aux objets connectés.



Faute d'une adoption de grande ampleur par la communauté des développeurs, le groupe Internet revient à l'assaut avec un nouvel OS léger baptisé Android Things qui n'est autre qu'une mouture améliorée de Brilllo. En rassemblant leurs compétences, **Google** et de Qualcomm souhaitent offrir aux développeurs des environnements de connectivité familiers: réseaux cellulaires, Wi-Fi, Bluetooth, prise en charge d'un large éventail de capteurs, caméras, cartes graphiques, sécurité matérielle, services **Google**, intégration du Cloud, etc. Jeffery Torrance, vice-président du développement des affaires de Qualcomm Technologies, a déclaré que « depuis le lancement du premier téléphone Android, Qualcomm et **Google** ont collaboré étroitement pour créer de nouvelles opportunités intéressantes pour les développeurs de mobiles, de portables et d'IoT ». Aujourd'hui le projet est beaucoup plus abouti et **Android Things** est accompagné d'Android Studio, des services **Google** Play, de la **Google** Cloud Platform et du SDK Android. **Google** fait remarquer qu'il existe déjà du hardware pour cela: **Android Things** est compatible avec Intel Edison, NXP Pico et Raspberry Pi 3.

Weave, bientôt sur Android et. iOS!

Il s'agit également d'un système d'exploitation temps réel (RTOS), domaine où la concurrence est rude avec une myriade d'alternatives: Contiki (disponible gratuitement sous licence BSD) et TinyOS.La firme annonce avoir aussi mis à jour sa plateforme Weave permettant aux objets connectés déjà sur le marché de profiter de ses services, à l'instar de **Google** Assistant.
Pour rappel, Weave fournit l'infrastructure cloud qui permet de relier les objets connectés entre eux et à Internet.
Dans un effort d'harmonisation des approches de standardisation, l'Open Interconnect Consortium et l'AllSeen Alliance regroupent des myriades de sociétés IT accompagner l'essor de l'IoT. Le kit de développement (SDK) Weave Device vient d'être introduit.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Google présente son nouvel OS pour objets connectés – Android Things

Devenir délégué à la protection des données | CNIL

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

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

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

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

A retenir

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

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

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

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

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

Qui peut être délégué à la protection des données ?

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

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

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

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

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

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

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

Lignes directrices du G29

> Guidelines on Data Protection Officers ('DPOs')

> WP243 ANNEX – Frequently asked questions

La version française de ces documents sera disponible début 2017.

Réagissez à cet article

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