La Chine lance sa loi sur la cybersécurité. Les entreprises sont inquiètes

	La Chine lance sa loi sur la cybersécurité. Les entreprises sont inquiètes

La Chine applique à partir de jeudi sa loi sur la cybersécurité, renforçant encore sa « Grande muraille » informatique, mais des entreprises étrangères s'inquiètent de l'impact de la nouvelle réglementation sur leurs activités.

Cette loi adoptée en novembre dernier ambitionne de protéger les réseaux chinois et les informations personnelles des utilisateurs, à l'heure où le rançongiciel WannaCry a rappelé la vulnérabilité des Etats face aux cyberattaques.
Mais des entreprises ont réclamé au gouvernement chinois un report de l'application de la loi. Elles s'inquiètent notamment des dispositions imprécises du texte et de l'influence qu'il pourrait avoir sur l'informatique dématérialisée (le « cloud ») et le traitement des données personnelles.
Les autorités semblent toutefois vouloir finaliser les règles.
Mi-mai, le directeur de l'Administration chinoise de la cybersécurité (CAC), Zhao Zeliang, a réuni 200 représentants d'entreprises et d'associations professionnelles locales et étrangères au siège de son organisme à Pékin.
La discussion était centrée sur les règles de transfert des données personnelles à l'étranger, ont rapporté des participants à l'AFP. Selon eux, les personnes présentes ont reçu une version actualisée de dispositions de la loi, et l'assurance de M. Zhao que certains des passages les plus polémiques seraient retirés.
Le nouveau document, consulté par l'AFP, ne fait par exemple plus mention de l'obligation controversée pour les entreprises de conserver en Chine les données personnelles de leurs clients.
Mais les appréhensions demeurent.
Les autorités « ne sont pas prêtes » à faire appliquer la loi et il est « très improbable » qu'un changement concret dans la législation intervienne dès le 1er juin, a assuré à l'AFP un participant qui a requis l'anonymat en raison de la sensibilité du dossier.
La Chine surveille déjà drastiquement l'internet, en bloquant les sites qu'elle estime politiquement sensibles, un système surnommé « la Grande muraille électronique » qui n'a toutefois pas empêché des universités et stations-services du pays d'être touchées par l'attaque planétaire du virus WannaCry.
La nouvelle loi sur la cybersécurité interdit aux internautes de publier tout contenu portant atteinte à « l'honneur national », « troublant l'ordre économique et social » ou destiné à « renverser le système socialiste », c'est-à-dire le Parti communiste au pouvoir.
Des entreprises étrangères craignent que la nouvelle loi entrave leur accès au marché chinois…[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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *La Chine lance sa loi sur la cybersécurité, les entreprises inquiètes – Le Parisien*

Qui a le droit d’accéder à nos données numériques après notre mort ?

Qui a le droit d’accéder à nos données numériques après notre mort ?

Faisant partir de la Loi du 7 octobre 2016 pour une République numérique
le 10 10 2016 (dite aussi Loi Lemaire), en complément d'un chapitre traitant de mesures sur l'ouverture des données publiques, d'un autre sur le principe de neutralité des réseaux et de portabilité des données, un chapitre traite de notre mort numérique ou en d'autres termes, après notre mort, qui pourra avoir accès aux données numériques qui nous appartenaient ?

La loi n° 78-17 du 6 janvier 1978 a été impactée par cette Loi pou rune république numérique.
L'article 40 est ainsi complété par un article 40-1 ainsi rédigé :
Art. 40-1 article I. : « Les droits ouverts à la présente section s'éteignent au décès de leur titulaire. Toutefois, ils peuvent être provisoirement maintenus conformément aux II et III suivants.

Art. 40-1 article II. : « Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.
« Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.
« Les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.
« Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.
« Les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés à la présente section. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel.
« Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect de la présente loi.
« La personne peut modifier ou révoquer ses directives à tout moment.
« Les directives mentionnées au premier alinéa du présent II peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés.
« Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite.

Art. 40-1 article IIII.-En l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés à la présente section dans la mesure nécessaire :
• «-à l'organisation et au règlement de la succession du défunt. A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ;
• «-à la prise en compte, par les responsables de traitement, de son décès. A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.
« Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en application du troisième alinéa du présent III.
« Les désaccords entre héritiers sur l'exercice des droits prévus au présent III sont portés devant le tribunal de grande instance compétent.
« IV.-Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne. » ;

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

---

Réagissez à cet article

Source : *LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique | Legifrance*

La Cnil veut protéger de manière effective les données des élèves

	La Cnil veut protéger de manière effective les données des élèves

La Commission nationale de l'informatique et des libertés (Cnil) veut fixer un cadre de régulation face au développement des offres de services numériques dans l'éducation.

Un appel à garantir la protection des données scolaires

Avec l'utilisation croissante des services numériques à l'école, la Cnil sollicite une action du ministère de l'Éducation nationale. La **Commission nationale de l'informatique et des libertés** appelle en effet la place Grenelle à garantir *« de façon effective et contraignante »* la protection des données scolaires. Dans un communiqué reçu ce mercredi, elle estime qu'il est *« plus que jamais nécessaire »* de fixer un cadre de régulation pour une protection de manière effective des données personnelles des élèves et des enseignants. Elle a notamment cité le **développement des offres de services numériques dans l'éducation** par les Gafam. Cet acronyme désignant les plus grands fournisseurs du web regroupe Google, Apple, Facebook, Amazon, Microsoft.

L'importance du respect des droits des personnes

Déjà annoncée au printemps 2016, cette **charte de confiance** est encore en cours de finalisation. La **Cnil** insiste alors sur le respect des droits des personnes. Selon elle, cette charte devrait garantir *« la non-utilisation des données scolaires à des fins commerciales, l'hébergement de ces données en France ou en Europe »*, rapporte *Europe1*. *« L'obligation de prendre des mesures de sécurité conformes aux normes en vigueur »* est également sollicitée…[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

---

Réagissez à cet article

Source : *Education: la Cnil veut protéger de manière effective les données des élèves – LINFO.re – France, Société*

Règlement européen RGPD : se préparer en 6 étapes avec la CNIL

	Règlement européen RGPD : se préparer en 6 étapes avec la CNIL

Le 25 mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

1. DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

> En savoir plus

2. CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

> En savoir plus

3. PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

> En savoir plus

4. GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

> En savoir plus

5. ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

> En savoir plus

6. DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

> En savoir plus

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

---

Réagissez à cet article

Source : *Règlement européen : se préparer en 6 étapes | CNIL*

RGPD : moins d'un an pour se mettre en conformité

RGPD : moins d'un an pour se mettre en conformité

Depuis le 25 mai dernier, les entreprises ont un peu plus de 11 mois pour se mettre en conformité avant l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD). Alors que le délai est relativement court, une récente étude du cabinet Vanson Bourne pour Compuware révèle que seules 43 % des organisations françaises disposent d'un plan complet pour s'adapter à ce règlement européen.

Pour Gerard Allison, Vice-Président EMEA chez Gigamon, il est essentiel que toutes les organisations s'y préparent dès à présent, aussi bien pour échapper aux sanctions que pour se protéger des hackers :
« Tout non-respect du RGPD exposera les entreprises à des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial. En outre, alors que ce nouveau règlement est une avancée positive dans la protection des données, les organisations doivent avoir conscience que les cybercriminels peuvent profiter de la situation en utilisant de nouvelles méthodes. Comme l'ont démontré les récents événements liés à l'attaque WannaCry, le ransomware est une technique largement utilisée par les hackers, qui évolue et peut devenir encore plus dangereuse, notamment si un pirate réussit à accéder à un réseau et que l'organisation ciblée n'a pas les outils nécessaires en place pour détecter la faille, ou simplement pour la signaler. Il pourrait alors, par exemple, menacer de la dénoncer auprès de la CNIL pour non-conformité, si elle ne paie pas la rançon. Est-il possible qu'une entreprise puisse préférer acheter le silence d'un hacker plutôt que de payer une amende pour ne pas avoir respecté le règlement ?
Ainsi, pour éviter de se retrouver en mauvaise posture et être en phase avec le RGPD, les organisations devront être capables de détecter, se protéger, prédire et contenir les menaces au cœur de leur réseau. Cela leur permettra notamment de répondre à l'obligation de signaler toute vulnérabilité dans les 72 heures au plus tard après en avoir pris connaissance, et de sauvegarder les données de leurs clients dans un endroit sûr. Et pour y parvenir, elles auront besoin d'une visibilité complète sur toutes les données qui transitent sur leurs réseaux, puisqu'on ne peut pas sécuriser ce qu'on ne voit pas…[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

---

Réagissez à cet article

Source : *RGPD : 365 jours pour se conformer – Global Security*

Des banques autorisées par la Cnil à tester la reconnaissance vocale

Des banques autorisées par la Cnil à tester la reconnaissance vocale

La Cnil indique avoir autorisé neuf établissements bancaires à expérimenter la reconnaissance vocale pour s'authentifier lors d'une connexion à un compte ou pour effectuer certaines transactions.

Lorsque vous vous connectez à votre compte bancaire, vous entrez certainement le numéro de votre compte, un mot de passe et éventuellement d'autres informations, comme votre code postal, pour être redirigé sur votre caisse régionale. Quand vous effectuez un virement bancaire ou un paiement quelconque, peut-être validez-vous la transaction en tapant un code. Ces méthodes d'authentification mises en place pour s'assurer que c'est bien vous qui cherchez à accéder au compte ou qui donnez certains ordres ne sont pas la panacée en matière de sécurité informatique mais elles ont le mérite d'être familières pour le grand public et facilement renouvelables en cas de besoin. Or aujourd'hui, elles sont concurrencées par la biométrie…[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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Neuf banques autorisées par la Cnil à tester la reconnaissance vocale – Business – Numerama*

---

10 règles à respecter pour utiliser un drone en toute sécurité

---

1. Ne pas survoler les personnes
2. Respecter les hauteurs maximales de vol
3. Ne pas perdre de vue son drone, ne pas l'utiliser de nuit
4. Ne pas utiliser son drone au-dessus de l'espace public en agglomération
5. Ne pas utiliser son drone à proximité d'un aérodrome
6. Ne pas survoler de sites sensibles ou protégés
7. Respecter la vie privée des autres
8. Ne pas diffuser les prises de vue sans l'accord des personnes concernées et ne pas en faire une utilisation commerciale
9. Vérifier les conditions d'assurance
10. Se renseigner en cas de doute

L'utilisation d'une caméra

Les prises de vue (photos ou vidéos) sont possibles en aéromodélisme dès lors que ces **prises de vue sont réalisées sans usage commercial ou professionnel.**

Le droit à la vie privée des autres personnes doit être respecté. **Les personnes présentes doivent être informées** si l'aéromodèle est équipé d'une caméra ou de tout autre capteur susceptible d'enregistrer des données les concernant.

Par ailleurs, **toute diffusion d'image permettant de reconnaître ou identifier les personnes (visages, plaques d'immatriculation …) doit faire l'objet d'une autorisation** des personnes concernées ou du propriétaire dans le cas d'un espace privé (maison, jardin etc.) et doit respecter la législation en vigueur (notamment la **loi du 6 janvier 1978 modifiée dite « Informatique et Libertés »**).

La violation de la vie privée est passible d'un an d'emprisonnement et 45 000 euros d'amende…[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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Réagissez à cet article

Source : *Quelle réglementation pour les drones en 2017 ?*

Les victimes de Cyberattaque sont aussi responsables de manquement à leur obligation de sécurité

	Les victimes de Cyberattaque sont aussi responsables de manquement à leur obligation de sécurité

Demain, les sociétés victimes d'une cyberattaque pourront être plus facilement attaquées en responsabilité par les clients lésés. Ce sera la double peine…

Difficile d'échapper à la nouvelle, les médias ont largement relayé l'information de la cyberattaque à large échelle perpétrée en fin de semaine dernière. Cette attaque a pris la forme pernicieuse d'un « ransomware », c'est-à-dire d'un cryptage de données couplé à une demande de rançon. Et gare à ceux qui ne voulaient pas obéir, la menace d'une destruction des données concernées était supposée les ramener dans le droit chemin.
Selon les informations disponibles par les médias, l'attaque aurait visé des entreprises qui utilisaient encore l'ancien système d'exploitation Windows XP, un système pour lequel Microsoft avait cessé de proposer des mises à jour depuis peu de temps. Mais comme le fait remarquer l'avocat Adrien Alberini au journal suisse Le Temps, cette situation complexe donne lieu à ce qu'on peut qualifier de « paradoxe de la cyberattaque »: aussi surprenant que cela puisse paraitre, les entreprises cibles d'une cyberattaque s'exposeront au final à un risque de sanctions significatives.
Ce paradoxe – la victime doublement victime en quelque sorte – s'explique en réalité par le renforcement du droit de la protection des données. Mais ces nouvelles exigences en matière de protection de données ne seront pas faciles à respecter, d'où le risque d'une attaque en responsabilité pour les entreprises victimes d'une cyberattaque. En bref, peu de chefs d'entreprises le savent, mais une réglementation modernisée en matière de protection des données – dénommée GDPR (General Data Protection Regulation) – entrera en vigueur l'année prochaine en Europe…[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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cyberattaque: le paradoxe de la double peine pour les entreprises – High-tech – Trends-Tendances.be*

Les drones civils aussi devront répondre au concept de « Privacy by Design »

	Les drones civils aussi devront répondre au concept de « Privacy by Design »

D’ici un an, les opérateurs de drones comme les fabricants, auront l’obligation de mettre en œuvre des « mesures techniques et opérationnelles appropriés » afin protéger les droits des personnes et des données. Laurent Archambault, avocat à la Cour, explique ici comment les acteurs de la filière drone, en Europe à partir du 25 mai 2018, devront non seulement acheter ou concevoir des drones qui prennent en compte cette question, planifier leurs missions dans cet état d’esprit, mais aussi adopter une organisation qui permette une protection maximisée des tiers et de leurs données.

Les drones sont par essence des appareils permettant des prises de vue ou la captation de données, discrètement. La grande majorité de ces aéronefs est de petite taille. Ils peuvent voler près du sol, longer des édifices ou encore suivre une personne de jour comme de nuit. Comme souligné par Edouard Geffray, Secrétaire général de la CNIL, la problématique du drone pour la vie privée et la protection des données réside d’ailleurs, non pas tant dans l’emport de capteurs, mais bien dans la mobilité et la discrétion du drone.
A cet égard, le concept de « *Privacy by Design* » pourrait constituer un moyen de limiter, voire de supprimer tant les atteintes à la vie privée que la captation de données personnelles par drone (ces dernières pouvant être grossièrement définies, comme des «*données non anonymes* »). Insistons sur le fait qu’à l’ère du numérique, ces deux domaines sont poreux entre eux..[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d’articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

---

Réagissez à cet article

Source : *Le concept de « Privacy by Design » à la rescousse des drones civils européens – Aerobuzz*

Données personnelles : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »

	RGPD : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »

A un an de l'entrée en vigueur du règlement européen sur la protection des données. Alice de La Mure, juriste au service Correspondants informatiques et libertés de la CNIL, revient sur les nouvelles obligations qui concernent largement les collectivités territoriales

Le règlement général sur la protection des données (RGPD), adopté par le Parlement européen le 14 avril 2016, sera directement applicable dans les Etats membres le 25 mai 2018. Il sera alors le texte de référence concernant la protection des données à caractère personnel. Il consolide, voire renforce, les grands principes de la loi Informatique et Libertés.
Divers axes s'en dégagent, dont plusieurs concernent directement les collectivités territoriales :
• la responsabilisation globale de l'ensemble des acteurs ;
• le renforcement des droits des personnes, avec notamment l'avènement du droit à la portabilité et du droit à la limitation du traitement ;
• l'augmentation du montant des sanctions susceptibles d'être prononcées par la CNIL : la loi du 7 octobre 2016 pour une République numérique avait …[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

---

Réagissez à cet article

Source : *Données personnelles : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »*