

# La police utilise les empreintes des cadavres pour débloquer les iPhone

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

x

x

x

x

x

x

x

La police utilise les empreintes des cadavres pour débloquer les iPhone

**Plusieurs sources dans les autorités policières américaines ont admis à Forbes utiliser les empreintes des corps pour débloquer les iPhone grâce au Touch ID, dans le cadre d'une enquête criminelle.**

La police cherche maintenant à savoir comment ils peuvent utiliser la reconnaissance faciale Face ID pour pirater les téléphones des suspects. Bob Moledor, spécialiste judiciaire au FBI, a déclaré à Forbes que la première utilisation connue du Touch ID dans une enquête criminelle remonte à 2016, après l'attaque terroriste dans l'université d'Etat de l'Ohio d'Abdul Razak Ali Artan, abattu ensuite par un policier. Moledor a confirmé qu'un agent du FBI a placé l'index du décédé sur son iPhone dans le but d'accéder à son téléphone et de révéler davantage d'informations sur ses motivations. Malheureusement, la tentative a été infructueuse car, pendant que le FBI demandait l'autorisation pour accéder au téléphone, il s'est éteint, ce qui signifie qu'un code était également nécessaire...[lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, twitter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à se mettre en conformité avec la réglementation numérique (dont le RGPD) et à se protéger des pirates informatiques.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)
- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES
- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous



Source : *La police utilise les empreintes des cadavres pour débloquer les iPhone*

---

## **L'OPAC de l'Oise met en conformité réglementaire ses accès Internet**

✕	<b>L'OPAC de l'Oise met en conformité réglementaire ses accès Internet</b>
---	----------------------------------------------------------------------------

---

**L'OPAC de l'Oise a déployé la passerelle de sécurité web d'Olfeo pour garantir le respect des règles d'usage d'internet par ses collaborateurs.**

Le bailleur social OPAC de l'Oise gère 31 532 logements dans 231 communes non seulement de l'Oise mais aussi de la Somme, de l'Aisne, du Val d'Oise et de Seine et Marne. Il dispose pour cela de 12 antennes de gestion réparties sur son territoire avec 670 collaborateurs en tout dont 600 sont informatisés et ont accès à Internet. Dans le cadre d'une modernisation plus globale, l'OPAC a souhaité moderniser sa sécurité d'accès au web, notamment pour garantir un respect réglementaire (blocage d'accès aux sites réalisant l'apologie du terrorisme, de la pédopornographie, etc.) mais pas seulement...[lire la suite]

---

**LE NET EXPERT**

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
  - **ANALYSE DE VOTRE ACTIVITÉ**
  - **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
    - **IDENTIFICATION DES RISQUES**
    - **ANALYSE DE RISQUE (PIA / DPIA)**
  - **MISE EN CONFORMITÉ RGPD** de vos traitements
  - **SUIVI** de l'évolution de vos traitements
    - **FORMATIONS / SENSIBILISATION :**
      - **CYBERCRIMINALITÉ**
  - **PROTECTION DES DONNÉES PERSONNELLES**
    - **AU RGPD**
    - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
  - **ORDINATEURS (Photos / E-mails / Fichiers)**
  - **TÉLÉPHONES** (récupération de **Photos / SMS**)
    - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
  - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
    - **SÉCURITÉ INFORMATIQUE**
  - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

**Besoin d'un Expert ? contactez-nous**

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *L'OPAC de l'Oise met en conformité réglementaire ses accès Internet*

# Comprendre et mettre en application le RGPD, objet de nos formations

<input type="checkbox"/>	Comprendre et mettre en application le RGPD, objet de nos formations
--------------------------	----------------------------------------------------------------------

**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.**

Comme nous l'avons détaillé sur notre page dédiée (Formation RGPD : Ce n'est pas qu'une affaire de juristes), les 6 étapes recommandées par la CNIL pour vous préparer au RGPD sont :

- 1- DÉSIGNER UN PILOTE
- 2- CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES
- 3- PRIORISER LES ACTIONS À MENER
- 4- GÉRER LES RISQUES
- 5- ORGANISER LES PROCESSUS INTERNES
- 6- DOCUMENTER LA CONFORMITÉ



A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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 étapes

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 : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles



Réagissez à cet article

---

**Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes***

# Formation RGPD/DPO : Concrètement, comment se mettre en conformité avec le règlement ?

Formation RGPD/DPO :  
Concrètement, comment se  
mettre en conformité avec  
le règlement ?

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



---

## Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

---

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

*« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».*

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



**Quelques articles sélectionnés par nos Experts :**

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la



Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

---

Réagissez à cet article

---

---

# Faille de sécurité chez Lenovo

✖	Faille de sécurité chez Lenovo
---	-----------------------------------

---

Sur certains modèles Lenovo, le lecteur d'empreinte ouvre une faille de sécurité potentielle. (CCM) – C'est une faille de sécurité importante que vient de révéler Lenovo. Le système de reconnaissance d'empreintes digitales de certains modèles de la marque laisse un accès aux mots de passe et aux identifiants de connexion.

Cette faille sur le lecteur d'empreinte du clavier a été découverte par un chercheur en sécurité de l'entreprise Security Compass. Le problème concerne plusieurs modèles d'ordinateurs PC Lenovo, comme les portables ThinkPad, ThinkCentre et ThinkStation qui tournent sous Windows 7, 8 et 8.1. Après une année 2015 compliquée pour la marque, Lenovo connaît de nouveaux problèmes de sécurité. Tout vient du **Lenovo Fingerprint Manager Pro**. Ce logiciel permet l'identification d'empreintes, à la manière de ce que fait le TouchID de l'iPhone. Il sert à l'identification des utilisateurs du PC, et il peut aussi être utilisé pour des identifications sur différents sites web...[lire la suite]

Les utilisateurs sont donc invités à installer la **version 8.01.87 de Fingerprint Manager Pro** pour résoudre ce problème.

#### LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)
  - ANALYSE DE VOTRE ACTIVITÉ
  - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
    - IDENTIFICATION DES RISQUES
    - ANALYSE DE RISQUE (PIA / DPIA)
  - MISE EN CONFORMITÉ RGPD de vos traitements
    - SUIVI de l'évolution de vos traitements
      - FORMATIONS / SENSIBILISATION :
        - CYBERCRIMINALITÉ
    - PROTECTION DES DONNÉES PERSONNELLES
      - AU RGPD
      - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
    - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - SÉCURITÉ INFORMATIQUE
  - SYSTÈMES DE VOTES ÉLECTRONIQUES

#### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *Faille de sécurité chez Lenovo*

# Le RGPD (GDPR en anglais) : une réglementation que doivent aussi suivre vos sous-traitants



Le RGPD (GDPR en anglais) : une réglementation que doivent aussi suivre vos sous-traitants



Le nouveau règlement européen sur la protection des données personnelles doit entrer en vigueur en mai 2018. Les donneurs d'ordre des métiers de service ont préparé leur mise en conformité et pressent leurs sous-traitants de faire de même. Cela représente pour eux de nouvelles charges à assumer.

**Denis JACOPINI nous rappelle un extrait des termes de l'article 28 du RGPD (Règlement Européen sur la Protection des Données) :**

*Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.*

*Le traitement par un sous-traitant est régi par un contrat [...] prévoit, notamment, que le sous-traitant:*

- a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;*
- b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;*
- c) prend toutes les mesures requises en vertu de l'article 32;*
- d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant;*
- e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;*
- f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant;*
- g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel; et*
- h) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.*

*En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.*

Ainsi, même si vous êtes en règle vis à vis du RGPD mais si votre sous-traitant ne l'est pas, le résultat pourrait bien être équivalent comme si vous n'étiez pas en règle.

La mise en conformité du sous-traitant requiert d'abord une mise à niveau des mesures organisationnelles et techniques de cyber sécurité, avant de se concentrer sur la gestion des données personnelles. Les PME et ETI ont souvent fait l'impasse sur ce domaine générateur de coûts, pensant, grâce à leur petite taille, d'échapper aux attaques les plus graves. Aujourd'hui avec les puissants moyens d'information, ce n'est plus le cas, un pirate peut appréhender une filière et frapper le maillon le plus faible...[lire la suite]

#### LE NET EXPERT

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
  - ANALYSE DE VOTRE ACTIVITÉ
  - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
    - IDENTIFICATION DES RISQUES
    - ANALYSE DE RISQUE (PIA / DPIA)
  - MISE EN CONFORMITÉ RGPD de vos traitements
    - SUIVI de l'évolution de vos traitements
    - **FORMATIONS / SENSIBILISATION :**
      - CYBERCRIMINALITÉ
    - PROTECTION DES DONNÉES PERSONNELLES
      - AU RGPD
      - À LA FONCTION DE DPO
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
  - SYSTÈMES NUMÉRIQUES
- **EXPERTISES & AUDITS** (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
  - SÉCURITÉ INFORMATIQUE
  - SYSTÈMES DE VOTES ÉLECTRONIQUES

#### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *Le GDPR, un risque pour les PME en position de sous-traitance ?*

---

## **Formation RGPD : Ce n'est pas qu'une affaire de juristes**

✖	<b>Formation RGPD : Ce n'est pas qu'une affaire de juristes</b>
---	-----------------------------------------------------------------

---

Le 25 mai 2018, le règlement européen sera appliqué. 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.

Les 6 étapes recommandées par la CNIL pour vous préparer au RGPD sont :

- 1- MESURER UN FAISSETTE**  
Pour évaluer la pertinence des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui assurera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. Et attendez 2018, une bonne d'ores et déjà déployer en « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.
- 2- CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES**  
Pour assurer 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.
- 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.
- 4- GÉRER LES RISQUES**  
En cas de non-conformité des traitements de données personnelles susceptibles d'exposer des risques élevés pour les droits et libertés des personnes concernées, vous devez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (AIP).
- 5- ORGANISER LES PROCESSUS INTERNES**  
Pour assurer la mise en œuvre de la protection des données par vos personnes, mettez en place des procédures internes qui garantiront la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des documents qui peuvent servir de base de la vie d'un traitement (sauf la politique de sécurité, gestion des données de participation ou d'accès, modification des données collectées, changement de prestataires).
- 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 résumés et actualisés régulièrement pour assurer une protection des données en continu.

Pour cartographier vos traitements de données personnelles, vous devez avoir un référentiel des outils, identifier des informations à la fois techniques et organisationnelles.  
Pour prioriser les actions à mener, vous devez identifier précisément les traitements à risque, les données sensibles et connaître les solutions techniques applicables.  
Pour gérer les risques, vous devez appliquer une méthode structurée à votre obligation. Prenez de la méthode RGPD, l'analyse d'impact relative à la protection des données (AIP) est le passage obligatoire pour tout organisme (entreprise ou association) émetteur de données sensibles appartenant à des tiers.  
L'organisation des processus internes nécessite une excellente connaissance des besoins et des risques. Une certification relative à une norme ISO 27001 ou ISO 9001 vous paraît essentielle.

Vous pouvez donc constater que pour chaque point ci-dessus, le chef d'orchestre que doit être le DPO doit à la fois avoir une bonne connaissance du règlement européen RGPD (ou GDPR en anglais) mais également connaître et maîtriser différents sujets tels que la sécurité informatique, différentes méthodes telles que l'analyse des flux de données et l'analyse de risques.

Enfin, nous constatons qu'il serait intéressant d'établir la liste de contacts avec le RGPD des établissements sous votre contrôle s'il est possible d'être contacté par un conseil juridique spécialisé en droit des données personnelles et d'une personne ayant une bonne connaissance de la sécurité informatique et de l'analyse de risques autour de vos données.

Voilà c'est ce que nous, conseillers pour les entreprises, nous recommandons.

---

Recevez-nous au prochain salon pour vous mettre en conformité avec le RGPD ?  
Recevez-nous au prochain salon pour apprendre à vous mettre en conformité avec le RGPD ?  
Contactez nous

---

**CONSEIL DE NOS PROFESSIONNELS**  
Nous ne sommes pas des professionnels impliqués respectivement d'être sanctionnés et par une demande réputation, le règlement européen (le RGPD) entrera en application le 25 mai 2018. Clarifiez les obligations que tous les professionnels devraient déjà respecter.  
Nous recommandons à nos clients de prendre les décisions appropriées de ce règlement européen et le mettre à l'œuvre pour continuer à exercer votre activité.

À lire aussi  
Mise en conformité RGPD : Note d'envoi  
Formation RGPD : l'essentiel sur le règlement européen pour la protection des données personnelles  
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 ?  
Commentaire du règlement européen sur les données personnelles en 6 étapes  
Notre sélection d'articles sur le RGPD (règlement européen sur la protection des données personnelles) et les DPO (délégué à la protection des données)

---

**NOTRE MISSION** : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.  
Par nos actions de formation, de sensibilisation et d'aide à la mise en œuvre de l'entreprise, nous faisons des professionnels 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 CNIL)  
Plan d'accompagnement sur : Formation RGPD : l'essentiel sur le règlement européen pour la protection des données personnelles

01 47 33 11 00  
02 47 33 11 00  
03 47 33 11 00  
04 47 33 11 00  
05 47 33 11 00  
06 47 33 11 00  
07 47 33 11 00  
08 47 33 11 00  
09 47 33 11 00  
10 47 33 11 00  
11 47 33 11 00  
12 47 33 11 00  
13 47 33 11 00  
14 47 33 11 00  
15 47 33 11 00  
16 47 33 11 00  
17 47 33 11 00  
18 47 33 11 00  
19 47 33 11 00  
20 47 33 11 00  
21 47 33 11 00  
22 47 33 11 00  
23 47 33 11 00  
24 47 33 11 00  
25 47 33 11 00  
26 47 33 11 00  
27 47 33 11 00  
28 47 33 11 00  
29 47 33 11 00  
30 47 33 11 00  
31 47 33 11 00  
32 47 33 11 00  
33 47 33 11 00  
34 47 33 11 00  
35 47 33 11 00  
36 47 33 11 00  
37 47 33 11 00  
38 47 33 11 00  
39 47 33 11 00  
40 47 33 11 00  
41 47 33 11 00  
42 47 33 11 00  
43 47 33 11 00  
44 47 33 11 00  
45 47 33 11 00  
46 47 33 11 00  
47 47 33 11 00  
48 47 33 11 00  
49 47 33 11 00  
50 47 33 11 00  
51 47 33 11 00  
52 47 33 11 00  
53 47 33 11 00  
54 47 33 11 00  
55 47 33 11 00  
56 47 33 11 00  
57 47 33 11 00  
58 47 33 11 00  
59 47 33 11 00  
60 47 33 11 00  
61 47 33 11 00  
62 47 33 11 00  
63 47 33 11 00  
64 47 33 11 00  
65 47 33 11 00  
66 47 33 11 00  
67 47 33 11 00  
68 47 33 11 00  
69 47 33 11 00  
70 47 33 11 00  
71 47 33 11 00  
72 47 33 11 00  
73 47 33 11 00  
74 47 33 11 00  
75 47 33 11 00  
76 47 33 11 00  
77 47 33 11 00  
78 47 33 11 00  
79 47 33 11 00  
80 47 33 11 00  
81 47 33 11 00  
82 47 33 11 00  
83 47 33 11 00  
84 47 33 11 00  
85 47 33 11 00  
86 47 33 11 00  
87 47 33 11 00  
88 47 33 11 00  
89 47 33 11 00  
90 47 33 11 00  
91 47 33 11 00  
92 47 33 11 00  
93 47 33 11 00  
94 47 33 11 00  
95 47 33 11 00  
96 47 33 11 00  
97 47 33 11 00  
98 47 33 11 00  
99 47 33 11 00  
100 47 33 11 00

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

# Prédictions cybersécurité 2018



Prédictions cybersécurité 2018

En 2018, les cybercriminels vont continuer à exploiter les faiblesses inhérentes à la nature humaine pour dérober des informations personnelles, avec des changements significatifs dans les techniques de cyberattaques. Découvrez les grandes lignes de ces tendances qui rythmeront l'année 2018 selon Proofpoint.

- ☒ L'email restera le vecteur de cyberattaque le plus utilisé
- ☒ Vol de cryptomonnaie : de nouvelles menaces aussi répandues que les chevaux de Troie
- ☒ Le facteur humain, toujours au cœur des cyberattaques
- ☒ La menace grandissante des bots sur les réseaux sociaux

[cliquez pour plus de détails]

---

#### LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)
  - ANALYSE DE VOTRE ACTIVITÉ
  - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
    - IDENTIFICATION DES RISQUES
    - ANALYSE DE RISQUE (PIA / DPIA)
  - MISE EN CONFORMITÉ RGPD de vos traitements
  - SUIVI de l'évolution de vos traitements
    - FORMATIONS / SENSIBILISATION :
      - CYBERCRIMINALITÉ
    - PROTECTION DES DONNÉES PERSONNELLES
      - AU RGPD
      - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
    - SYSTÈMES NUMÉRIQUES
  - EXPERTISES & AUDITS (certifié ISO 27005)
    - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
      - SÉCURITÉ INFORMATIQUE
    - SYSTÈMES DE VOTES ÉLECTRONIQUES

#### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

---



Réagissez à cet article

Source : *Prédictions cybersécurité 2018 – Global Security Mag Online*



---

# Mise en garde des utilisateurs de Google Home et autres enceintes « intelligentes »

✕	Mise en garde des utilisateurs de Google Home et autres enceintes « intelligentes »
---	-------------------------------------------------------------------------------------

---

Guidée vocalement, une enceinte connectée assiste l'utilisateur dans les tâches de son quotidien. Quels enjeux posent cette technologie au regard de la vie privée des utilisateurs ?

### Qu'est-ce qu'une enceinte connectée dite intelligente » ?

Une enceinte connectée « intelligente » est un dispositif équipé d'un haut-parleur et d'un micro qui intègre un assistant vocal. Grâce à cet équipement, l'enceinte est capable d'interagir avec l'utilisateur pour lui délivrer un service suite à une requête vocale. L'assistant est en mesure de répondre à une question, donner la météo, régler le chauffage, activer des lumières, réserver un VTC/Taxi, acheter des billets...

Le principe général de fonctionnement se caractérise par 4 grandes étapes :

Etape 1 – L'utilisateur « réveille » l'enceinte à l'aide d'une expression clé (« Hey Snips » / « Ok Google » / « Hey Alexa »).

Etape 2 – L'utilisateur énonce sa requête.

Etape 3 – La parole prononcée est automatiquement transcrite en texte puis interprétée afin qu'une réponse adaptée soit fournie.

Etape 4 – L'enceinte repasse en « veille»

Certaines de ces enceintes enregistrent localement les requêtes de l'utilisateur de manière à lui laisser la maîtrise de ses données (ex. une enceinte connectée avec l'assistant vocal de Snips). D'autres en revanche, envoient ces requêtes dans le cloud, autrement dit sur les serveurs de traitement de la société (ex. Amazon Echo, Google Home...). Dans les deux cas, l'appareil (ou ses serveurs) peut être amené à conserver :

- Un historique des requêtes transcrites afin de permettre à la personne de pouvoir les consulter et à l'éditeur d'adapter les fonctionnalités du service.
- Un historique des requêtes audio afin de permettre à la personne de les réécouter et à l'éditeur d'améliorer ses technologies de traitement de la parole.
  - Les métadonnées associées à la requête comme par exemple, la date, l'heure, le nom du compte.

[...]

#### Nos conseils

1. Encadrer les interactions de ses enfants avec ce type d'appareils (rester dans la pièce, éteindre le dispositif lorsqu'on n'est pas avec eux) ;
2. Couper le micro / éteindre l'appareil lorsque l'on ne s'en sert pas ou lorsqu'on ne souhaite pas pouvoir être écouté ;
3. Avertir des transcriptions de l'enregistrement potentiel des conversations (ou couper le micro lorsqu'il y a des invités) ;
4. Vérifier qu'il est bien réglé par défaut pour filtrer les informations à destination des enfants.
5. Connecter des services qui présentent réellement une utilité pour vous, tout en considérant les risques à partager des données intimes ou des fonctionnalités sensibles (ouverture porte, alarme) ;
6. Être vigilant sur le fait que les propos tenus face à l'appareil peuvent enrichir votre profil publicitaire ;
7. Ne pas hésiter à contacter les services supports en cas de questions et, le cas échéant, la CNIL.
8. Se rendre régulièrement sur le tableau de bord pour supprimer l'historique des conversations/questions posées et personnaliser l'outil selon vos besoins. Par exemple, définir le moteur de recherche ou la source d'information utilisé par défaut par l'assistant, lire la suite)

#### LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX - MISE EN CONFORMITÉ)
  - ANALYSE DE VOTRE ACTIVITÉ
  - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
  - IDENTIFICATION DES RISQUES
  - ANALYSE DE RISQUE (PIA / OPIA)
- MISE EN CONFORMITÉ RGPD de vos traitements
  - SUIVZ de l'évolution de vos traitements
  - FORMATIONS / SENSIBILISATION
  - CYBERCRIMINALITÉ
  - PROTECTION DES DONNÉES PERSONNELLES
    - AI RGPD
    - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmes/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
  - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JURIDIQUES | ADMINISTRATIVES
  - SÉCURITÉ INFORMATIQUE
  - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'Information & Informatique Légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DQSTFP (Numéro formateur n°93 84 89841 84).


☐

☐

Réagissez à cet article

Source : *Enceintes intelligentes : des assistants vocaux connectés à votre vie privée | CNIL*

# 7 règles simples pour protéger votre entreprise contre les cyber-attaques

 7 règles simples pour protéger votre entreprise contre les cyber-attaques

**Il ne se passe pas un jour sans que l'on entende parler de cyber-attaques, ce qui peut causer la détresse de certaines entreprises. Si de grandes entreprises telles que Merck ou Pizza Hut ne parviennent pas à empêcher des cyber-attaques, comment les autres peuvent-elles faire face ?**

Il ne se passe pas un jour sans que l'on entende parler de cyber-attaques, ce qui peut causer la détresse de certaines entreprises. Si de grandes entreprises telles que Merck ou Pizza Hut ne parviennent pas à empêcher des cyber-attaques, comment les autres peuvent-elles faire face ?

Ceci est bien entendu la mauvaise attitude à adopter. Bien que les grandes entreprises aient plus de ressources à leur disposition, beaucoup de violations de données sont la conséquence de simples failles de cyber-sécurité peu coûteuses à résoudre.

Vous trouverez ci-dessous 7 points que les entreprises devraient observer afin de limiter les risques de cyber-attaque.

1.

**Créer un mot de passe sûr**

2.

**Ne réutilisez pas et ne partagez pas vos mots de passe**

3.

**Sauvegardez vos fichiers importants**

4.

**Méfiez-vous des attaques d'hameçonnage**

5.

**Appliquez des "patches"**

6.

**Protégez vos biens matériels**

7.

**Organisez des formations de personnel**

Les problématiques listées ci-dessus devraient être abordées durant les formations de sensibilisation du personnel mais on ne peut attendre de la part des employés à ce qu'ils s'en souviennent après une seule formation. En effet, les employés devraient être formés au cours de leur intégration mais devraient également bénéficier de rappels annuels ou de formations ponctuelles lors d'incidents de sécurité. Des formations de sensibilisation du personnel régulières permettront aux employés de se souvenir des règles à suivre.

---

#### LE NET EXPERT

:

- FORMATIONS / SENSIBILISATION :
  - CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
  - AU RGPD
  - À LA FONCTION DE DPO
- MISE EN CONFORMITÉ RGPD / CNIL
  - AUDIT RGPD ET CARTOGRAPHIE de vos traitements
  - MISE EN CONFORMITÉ RGPD de vos traitements
  - SUIVI de l'évolution de vos traitements
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
    - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - SÉCURITÉ INFORMATIQUE
  - SYSTÈMES DE VOTES ÉLECTRONIQUES

**Besoin d'un Expert ? contactez-nous**

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

**Source : 7 règles simples pour protéger votre entreprise contre les cyber-attaques – IT Governance Blog FR**