

La CGPME sensibilise les PME à la cybersécurité | Denis JACOPINI

	La CGPME sensibilise les PME à la cybersécurité
---	---

La cybersécurité est un facteur de productivité, de compétitivité et donc de croissance pour les entreprises. Quelle que soit sa taille, une PME doit prendre conscience qu'elle peut être à tout moment confrontée à la cybercriminalité.

Qu'il s'agisse, par exemple, de malveillances visant à la destruction de données ou d'espionnage économique et industriel, les conséquences des attaques informatiques pour les entreprises, et plus particulièrement les TPE, sont généralement désastreuses et peuvent impacter leur pérennité. Pour la CGPME, chaque entreprise doit aujourd'hui se doter d'une politique de sécurisation des systèmes d'information inhérente à l'usage des nouvelles technologies. Si les contraintes financières des petites structures restent un frein à la construction d'une cybersécurité optimale, il existe des bonnes pratiques peu coûteuses et faciles à mettre en œuvre permettant de limiter une grande partie des risques liés à l'usage de l'informatique. Pour recenser ces usages, la Confédération, par le biais de sa Commission Economie Numérique, s'est rapprochée de l'ANSSI. Fruit d'un partenariat constructif, un guide des bonnes pratiques informatiques a été élaboré afin de sensibiliser les PME sur cette problématique tout en leur apportant les moyens opérationnels de préserver leurs systèmes d'information.

A vous désormais, chefs d'entreprises, de devenir les acteurs de votre propre sécurité !

François Asselin Président CGPME

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise. Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : Guide des bonnes pratiques CGPME/ANSSI
http://www.lenetexpert.fr/wp-content/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf

RGPD Règlement européen sur la protection des données : ce qui change pour les professionnels



RGPD Règlement
européen sur la
protection des données
: ce qui change pour les
professionnels

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne entrera en application le 25 mai 2018. L'adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique.

- Un cadre juridique unifié pour l'ensemble de l'UE
- Un renforcement des droits des personnes
- Une conformité basée sur la transparence et la responsabilisation
- Des responsabilités partagées et précisées
- Le cadre des transferts hors de l'Union mis à jour
- Des sanctions encadrées, graduées et renforcées
- Comment les autorités de protection se préparent-elles ?

Où trouver le texte officiel du RGPD (Règlement européen sur la protection des données) ?

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD** ? ?

Besoin d'une **formation pour apprendre à vous**

mettre en conformité avec le RGPD ?

Contactez-nous

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

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 ;



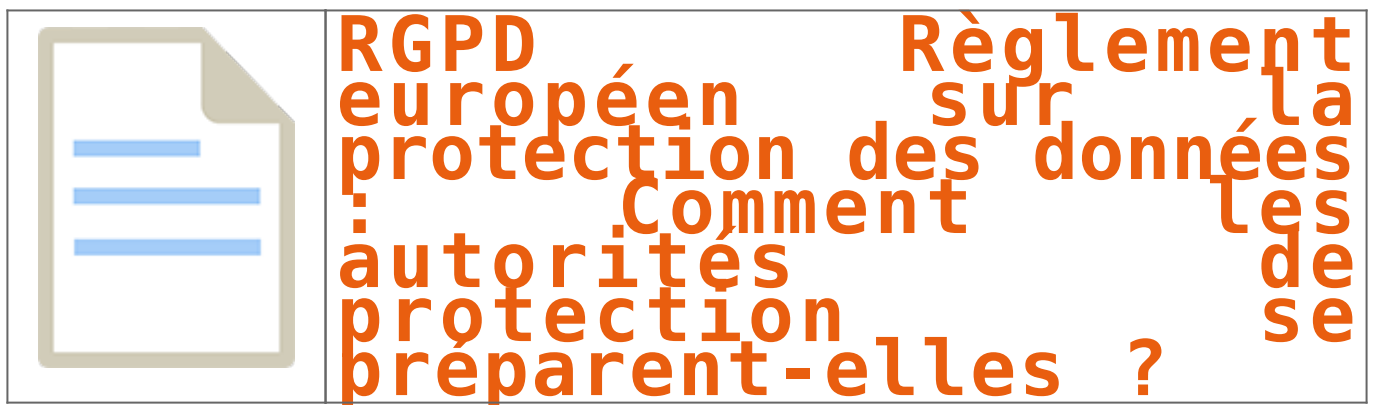
[Contactez-nous](#)



Réagissez à cet article

Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

RGPD Règlement européen sur la protection des données : Comment les autorités de protection se préparent-elles ?



Le G29

Dans son plan d'action 2016, adopté en février 2016, le G29 a présenté ses priorités pour permettre l'application effective du règlement en avril 2018. Plusieurs groupes de travail se sont déjà mis en place pour décliner ce plan d'action.

Les 4 objectifs principaux :

1. Préparer la mise en place du Comité européen de la protection des données (CEPD), qui remplacera le G29 en 2018 ;
2. Préparer la mise en place du guichet unique et le mécanisme coopération et de cohérence entre les autorités ;
3. Proposer des lignes directrices ou des bonnes pratiques aux professionnels pour **les 4 sujets prioritaires identifiés** : le droit à la portabilité, la certification, le délégué à la protection des données (DPO), les traitements à risque d'ici la fin de 2016 ;
4. Promouvoir et diffuser le règlement afin que l'ensemble des acteurs se l'approprie.

Le G29 prévoit également la consultation régulière des parties prenantes dans une démarche itérative sur deux ans afin d'enrichir sa réflexion.

Il a organisé le 26 juillet 2016 à Bruxelles des ateliers collaboratifs. Cet espace de concertation multi-acteurs a réuni les représentants de la société civile, des fédérations professionnelles, des universitaires et des institutions européennes, autorités de protection des données autour des 4 sujets prioritaires qu'il a identifiés.

Les échanges et propositions de cette journée ont permis au G29 d'alimenter les différents groupes de travail qu'il a déjà mis en place autour de ces mêmes thèmes. L'objectif étant de décliner d'ici 2018 les principes du règlement en mesures opérationnelles correspondant aux besoins et attentes des principaux acteurs concernés par la mise en œuvre du règlement.

D'autres consultations seront organisées sur d'autres thématiques.

La CNIL

La CNIL est très impliquée dans chacun des groupes de travail mis en place par le G29, dont elle assure la Présidence jusqu'en février 2018. Elle a proposé une consultation en ligne des acteurs français **sur ces mêmes sujets**.

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD** ? ?

Besoin d'une **formation pour apprendre à vous**

mettre en conformité avec le RGPD ?

Contactez-nous

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

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** ;



[Contactez-nous](#)

Réagissez à cet article

Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

Qu'est ce qu'un cybercriminel ?



Cette question a été posée à Denis JACOPINI par des étudiants. Ci-dessous une réponse succincte.

Avant de répondre à cette question, il est important de poser la définition de la cybercriminalité.

La définition qui selon moi définit le mieux la cybercriminalité est celle qui considère la cybercriminalité comme une **notion large qui regroupe toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau**. (Wikipedia)

Que ça soit dans le cas d'atteintes aux biens ou d'atteintes aux personnes, il est couramment décomposé 3 types d'infractions :

- **Les infractions spécifiques aux technologies de l'information et de la communication** : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements automatisés de données personnelles (comme la cession des informations personnelles), les infractions aux cartes bancaires, les chiffrements non autorisés ou non déclarés ou encore les interceptions.
- **Les infractions liées aux technologies de l'information et de la communication** : cette catégorie regroupe la pédopornographie, l'incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes, les atteintes aux biens.
- **Les infractions facilitées par les technologies de l'information et de la communication**, que sont les escroqueries en ligne, la contrefaçon ou tout autre violation de propriété intellectuelle.

Ainsi, un cybercriminel est une personne qui commet au moins une de ces 3 infractions.

Les principales motivations sont :

- Gagner de l'argent (ou ne pas en dépenser ce qui revient au même) en réalisant par exemple des actes de piratages d'œuvres intellectuelles telles que des musiques ou des films. D'autres peuvent aussi prendre le risque de chercher à en tirer des bénéfices soit en les revendant ces œuvres, en les mettant à disposition sur des sites internet mitraillant de publicités rémunérées leurs visiteurs ou permettant le téléchargement contre un appel vers un numéro surtaxé. D'autres vont réaliser des vols d'informations (Magasins TARGET en 2013), des blocages de systèmes informatiques (TVS Monde en 2015) ou des cryptages de fichiers en demandant à l'issue de l'opération une rançon en échange de tranquillité (Laboratoires Labio en 2015, Disney en 2017) ou de rétablir le système dans son état initial, une technique semblable à celles utilisées par la mafia (Pirates informatiques : des techniques très proches de la mafia – Gilles Fontaine) ;
- Terroriser la population en répandant des messages idéologiques (+ de 25000 sites Internet piratés diffusant un message pro islamiste à la suite des attentats de Charlie Hebdo) ou bien en coupant les ressources en électricité d'une population (Ukraine en 2015 et 2016) ;
- S'attaquer à un état dans un but politique (Attaque informatique de la centrale nucléaire de Bouchehr en Iran destinée à détruire des centrifugeuses d'enrichissement d'uranium en 2010) ou militaire (Attaque de la Georgie par la Russie en 2007) ou d'espionnage (Bercy en 2011) ;
- Dans un but de montrer ses capacités ou se lancer un défi (comme David Dennis en 1974). Débrouille-vous pour faire venir aux oreilles de hackers qu'un système informatique est inattaquable, vous verrez alors fleurir des volontaires masqués qui passeront leurs journées et leurs nuits à tenter de trouver la faille dans le but de prouver leur supériorité ;

Ainsi, selon moi, un cybercriminel est un individu qui commet avec ou sans intention une ou plusieurs infractions répréhensibles concernées par le champ couvert par la cybercriminalité, sans autorisation expresse du tiers concerné, quel que soit l'intention et l'objectif poursuivis.

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 DORTEFP (Numéro formateur n°93 84 63041 84).

Denis JACOPINI est Expert Juridique 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 ;
- **Conformité** (et sensibilisation) à la **Cybercriminalité** (autorisation n°93 84 63041 84) ;
- **Audits Sécurité** (ISO 27005) ;
- **Expertises techniques et judiciaires** ;
- **Recherche de preuves** : téléphones, disques durs, e-mails, contenus, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



Contactez-nous

Réagissez à cet article

Source : *Cybercrime – Wikipédia*

Le cadre légal de la géolocalisation des salariés | Denis JACOPINI



Le cadre légal de la géolocalisation des salariés

Afin de préserver la sécurité des véhicules et de leurs occupants, de plus en plus d'employeurs décident de recourir à la géolocalisation de leurs véhicules de société. Un procédé légal mais sous certaines conditions!

1. Que le dispositif soit mis en œuvre par l'entreprise ou par l'intermédiaire d'un prestataire, c'est à l'employeur que revient l'obligation de procéder à la déclaration auprès de la Commission nationale informatique et libertés (Cnil).
2. Cette déclaration doit notamment exposer les raisons et les objectifs auxquels répond le dispositif permettant la localisation des employés (lutte contre le vol, gestion des temps de parcours, par exemple). L'employeur doit nécessairement attendre le récépissé de déclaration délivré par la Cnil pour mettre en action son dispositif.
3. Selon les exigences de la Cnil, le traitement d'informations relatives aux employés doit être proportionné à la finalité déclarée, c'est-à-dire qu'il doit s'effectuer de façon adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi.
4. L'employeur doit informer ses employés (par courrier ou réunion d'information) de la mise en œuvre du dispositif de géolocalisation et des informations qui vont être collectées. À défaut, il s'expose à une amende de 1 500 euros. L'information doit porter sur l'identité et l'adresse du responsable du traitement, la ou les finalités du traitement, les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement, les destinataires de ces données (direction, services RH ou comptables), l'existence d'un droit d'accès et de rectification et d'opposition et leurs modalités d'exercice.
5. La non-déclaration de traitement à la Cnil par la société est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : <http://www.lefigaro.fr/automobile/2015/03/17/30002-20150317ARTFIG00284-le-cadre-legal-de-la-geolocalisation-des-salaries.php>
Par Me Rémy Josseume, avocat à la Cour, président de l'Automobile-Club des avocats

RGPD Règlement européen sur

la protection des données : Où trouver le texte ?

	<p>RGPD Règlement européen sur la protection des données Où trouver le texte ?</p>
---	---

Vous pouvez trouver le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données :

Sur le site de la CNIL ;

Sur le site de l'Union Européenne ;

Sur notre site.

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

Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?

Contactez-nous

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



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.




[Contactez-nous](#)

Réagissez à cet article

Source : Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL

RGPD Règlement européen sur la protection des données : Des sanctions encadrées, graduées et renforcées

	RGPD européen protection : Des encadrées, renforcées	Règlement sur la des données sanctions graduées et
---	---	---

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

Les autorités de protection peuvent notamment :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, **de 2% jusqu'à 4% du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.

Ce montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement pour le territoire de toute l'Union européenne.

Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de protection sera infligée à l'entreprise.

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

Besoin d'une formation pour apprendre à vous

mettre en conformité avec le RGPD ?

Contactez-nous

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

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** ;



[Contactez-nous](#)

Réagissez à cet article

Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

Comment est née la cybercriminalité ?



Cette question a été posée à Denis JACOPINI par des étudiants. Ci-dessous une réponse succincte.

Avant de répondre à cette question, il est important de poser la définition de la cybercriminalité.

La définition qui selon moi définit le mieux la cybercriminalité est celle qui considère la cybercriminalité comme une **notion large qui regroupe toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau.** (Wikipedia)

Que ça soit dans le cas d'atteintes aux biens ou d'atteintes aux personnes, il est couramment décomposé 3 types d'infractions :

- **Les infractions spécifiques aux technologies de l'information et de la communication** : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements automatisés de données personnelles (comme la cession des informations personnelles), les infractions aux cartes bancaires, les chiffrements non autorisés ou non déclarés ou encore les interceptions.
- **Les infractions liées aux technologies de l'informations et de la communication** : cette catégorie regroupe la pédopornographie, l'incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes, les atteintes aux biens.
- **Les infractions facilitées par les technologies de l'information et de la communication**, que sont les escroqueries en ligne, la contrefaçon ou tout autre violation de propriété intellectuelle.

En France la cybercriminalité est prise juridiquement en compte depuis la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, mais j'aurai tendance à penser que la cybercriminalité est née bien avant, bien avant l'informatique puisque dans la définition retenue, la notion d'informatique n'y est pas, il est fait mention de la notion de réseau (informatique mais aussi téléphonique...).

Ainsi, le premier cas d'infraction pénale que nous avons retrouvé est le détournement d'usage réalisé par John Draper, connu également sous le nom Captain Crunch, en 1969. Il parvint, à l'aide d'un sifflet qui possède la même tonalité que le réseau téléphonique américain, à passer des appels longues distance gratuitement lorsqu'il sifflait dans le combiné. Captain Crunch a été condamné pour ces actes à deux mois de prison en 1976. Les actes cybercriminels ont ensuite dans les années 80 évolué dans le monde informatique.

On pourrait ainsi conclure que même si la cybercriminalité doit son expansion à l'usage de plus en plus répandu de l'informatique, la cybercriminalité est née dans les années 60 au travers de piratages de lignes téléphoniques à partir d'un simple objectif propre aux êtres vivants : détourner l'environnement à son propre avantage.

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 DDRETF (Numéro formateur n°93 84 03041 84).

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



- **Mise 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, contenus, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contacter-nous](#)

Réagissez à cet article

Source : *Cybercrime – Wikipédia*

Comment se préparer aux incidents de sécurité ?



Comment
préparer
Incidents
sécurité ?

se
aux
de

Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.

Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.

Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

Les objectifs à atteindre

- 1. Plan de cybersécurité**
- 2. Gestion du risque**
- 3. Gestion de l'identité**
 - **Contrôle d'accès**
 - **Authentification**
 - **Autorisation**
 - **Responsabilité**
- 4. Surveillance de réseau**
- 5. Architecture de sécurité**
- 6. Contrôle des actifs, des configurations et des changements**
- 7. Cartographie de la gestion des incidents**

...[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>



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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Se préparer aux incidents de sécurité*

Un baccalauréat en cybersécurité à Polytechnique Montréal



Un baccalauréat en cybersécurité à Polytechnique Montréal

La Commission des études a approuvé la création d'un nouveau baccalauréat en cybersécurité qui sera offert à Polytechnique Montréal à l'automne 2017.

Les demandes pour un programme de formation en ligne en cybercriminalité, incluant des stages en entreprise, se sont faites pressantes au cours des dernières années et Polytechnique Montréal a décidé de créer un baccalauréat par cumul avec appellation en cybersécurité. La Commission des études de l'Université de Montréal a donné son approbation à ce projet à sa réunion du 21 mars.

Le nouveau programme permettra de combiner deux certificats liés à la thématique (cyberenquête, cyberfraude ou cybersécurité) avec un autre programme de 30 crédits de l'UdeM ou de HEC Montréal en vue de l'obtention d'un diplôme de baccalauréat. L'école de génie, rappellent les responsables, offre une formation en cybersécurité au premier cycle depuis 2007. Le projet vise à répondre «le plus adéquatement possible aux nouveaux besoins du marché du travail, qui est confronté à une pénurie de main-d'œuvre amplifiée par un taux de cybercriminalité en hausse exponentielle. De plus, la multiplication des supports mobiles ainsi que l'émergence de l'infonuagique posent de nouveaux défis».

Considérant qu'une proportion importante des étudiants de ces programmes ne possèdent pas de diplôme universitaire de premier cycle, et considérant le manque de main-d'œuvre dans ces domaines, «il apparaît essentiel que le diplôme de baccalauréat qui pourrait être décerné par cumul de certificats présente une dénomination spécifique [du] domaine d'études et de pratique, dans une perspective de valeur ajoutée, tant pour la formation que pour l'employabilité et la reconnaissance des entreprises qui emploient ces diplômés», fait valoir Polytechnique Montréal.

Le nouveau programme devrait voir le jour l'automne prochain.

(MATHIEU-ROBERT SAUVÉ)

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>



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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Un baccalauréat en cybersécurité à Polytechnique Montréal* | UdeMNouvelles