


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

	<b>RGPD européen protection : encadrées, renforcées</b>	<b>Règlement sur la des données sanctions graduées et</b>
---	---	---

---

**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 DDRTEFP (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 NIS2** ;
- 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 : *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 DRTTEF 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

---

# RGPD Règlement européen sur la protection des données : Le cadre des transferts hors de l'Union mis à jour



**Les responsables de traitement et les sous-traitants peuvent transférer des données hors UE seulement s'ils encadrent ces transferts avec des outils assurant un niveau de protection suffisant et appropriés des personnes.**

Par ailleurs, les données transférées hors Union restent soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.

Ainsi, et hormis les transferts fondés sur une décision d'adéquation de la Commission Européenne, les responsables de traitement et les sous-traitants peuvent mettre en place :

- des règles d'entreprises contraignantes (BCR) ;
- des clauses contractuelles types approuvées par la Commission Européenne ;
- des clauses contractuelles adoptées par une autorité et approuvées par la Commission européenne.

**De nouveaux outils sont également prévus :**

- pour les sous-traitants : la possibilité de mettre en place des règles d'entreprises contraignantes ;
- pour les autorités publiques : le recours à des accords contraignants ;
- pour les responsables de traitement et les sous-traitants : l'adhésion à des codes de conduite ou à un mécanisme de certification. Ces deux outils doivent contenir des engagements contraignants.

Enfin, une autorisation spécifique de l'autorité de protection basée sur ces outils n'est plus requise.

---

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*

# Les entreprises sont la

# première cible visée par la cybercriminalité | Denis JACOPINI

2

Les entreprises sont la première  
cible visée par la cybercriminalité

**ESET, pionnier en protection proactive depuis plus de deux décennies, vient de publier un rapport très complet sur les principales tendances pour 2015 en cybercriminalité.**

Alors que l'an dernier tout se concentrait autour de la protection de la vie privée sur Internet et les Malwares sur Android, de nouveaux secteurs de risques en sécurité informatique émergent en 2015.

Le rapport gratuit Tendances pour 2015, est axé sur les cinq principaux domaines sur lesquelles les entreprises doivent se concentrer pour combattre les attaques. Il explique pourquoi les entreprises doivent être sur leurs gardes, commente l'évolution des menaces et leur donne des conseils pour protéger au mieux leurs actifs.

"Alors que les organisations améliorent continuellement leurs connexions digitales, de nouvelles pistes s'ouvrent aux cybercrimes, " explique Benoît Grunemwald, Directeur Marketing et Commercial ESET France. "L'astuce est de faire en sorte que vos défenses soient plus impénétrables que celles des entreprises qui vous entourent. En comprenant mieux le paysage des menaces vous êtes bien mieux préparé pour contrer les choses indésirables qui se cachent autour de vous. "

**Le rapport est axé sur les principaux risques :**

1. L'évolution des APTs
2. Malware au point de vente
3. Fuite de l'information
4. Vulnérabilités
5. Doit-on se méfier des objets connectés ? Représentent-ils une menace ?

"Nous pouvons tous imaginer combien il est frustrant pour les entreprises de devoir continuellement protéger leurs actifs contre les pirates et les criminels, c'est pour cela que nous avons voulu leur fournir de l'aide avec ce rapport " commente Benoît Grunemwald. "Nous avons demandé à nos experts en sécurité de nous fournir une analyse détaillée de ce qu'ils pensent être des menaces émergentes. Ce rapport est destiné à fournir des informations supplémentaires aux organisations, à les aider à revoir leurs technologies et processus de sécurité et à mettre en place les ressources nécessaires aux endroits stratégiques. "

Le rapport détaillé peut être téléchargé sur : WeLiveSecurity

<http://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf>

Afin d'aider les entreprises à rester vigilantes et à se protéger contre les possibles tentatives d'intrusion de leur parc informatique, ESET protège les entreprises via ses solutions professionnelles. Une toute nouvelle génération arrive sur le marché fin février 2015, avec une architecture totalement revisitée...

Pour découvrir en avant-première les nouveautés des solutions et de la nouvelle console d'administration, il suffit de suivre la présentation sur le site internet ESET.

---

**À propos d'ESET :** Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public. Pionnier en matière de détection proactive des menaces véhiculées par l'Internet, ESET est aujourd'hui le leader dans ce domaine. À ce jour, l'#antivirus ESET Nod32 détient le record mondial de récompenses décernées par le laboratoire indépendant Virus Bulletin depuis 1998. ESET Nod32, #ESET Smart Security et ESET Cybersecurity pour Mac sont reconnus et appréciés par des millions d'utilisateurs dans le monde.

---

Expert Informatique 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 : <https://mail.google.com/mail/u/0/?hl=fr&shva=1###inbox/14be54b2709b0c02?compose=14be53ae312f08d7>

---

# **RGPD Règlement européen sur la protection des données : Des responsabilités partagées et précisées**



**RGPD Règlement  
européen sur la  
protection des données  
: Des responsabilités  
partagées et précisées**



Le règlement européen sur la protection des données vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations pesant sur les responsables de traitements et les sous-traitants.

### Le représentant légal

C'est le point de contact de l'autorité. Il a mandat pour « être consulté en complément ou à la place du responsables de traitement sur toutes les questions relatives aux traitements »

### Le sous-traitant

Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability. Il a notamment une obligation de conseil auprès du responsables de traitement pour la conformité à certaines obligations du règlement (PIA, failles, sécurité, destruction des données, contribution aux audits)

Il est tenu de maintenir un registre et de désigner un DPO dans les mêmes conditions qu'un responsable de traitement.

---

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 : Une conformité basée sur la transparence et la responsabilisation**



**RGPD Règlement  
européen sur la  
protection des données  
: Une conformité basée  
sur la transparence et  
la responsabilisation**

Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

### Une clé de lecture : la protection des données dès la conception et par défaut (*privacy by design*)

Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils devront veiller à limiter la quantité de données traitées dès le départ (principe dit de « minimisation »).

### Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (*accountability*).

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

### De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- le DPO (délégué à la protection des données)
- les études d'impact sur la vie privée (EIVP)

### Les « études d'impact sur la vie privée » (EIVP ou PIA)

Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

En cas de risque élevé, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

### Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

### Le Délégué à la Protection des données (*Data Protection Officer*)

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amènent à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

---

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 ;



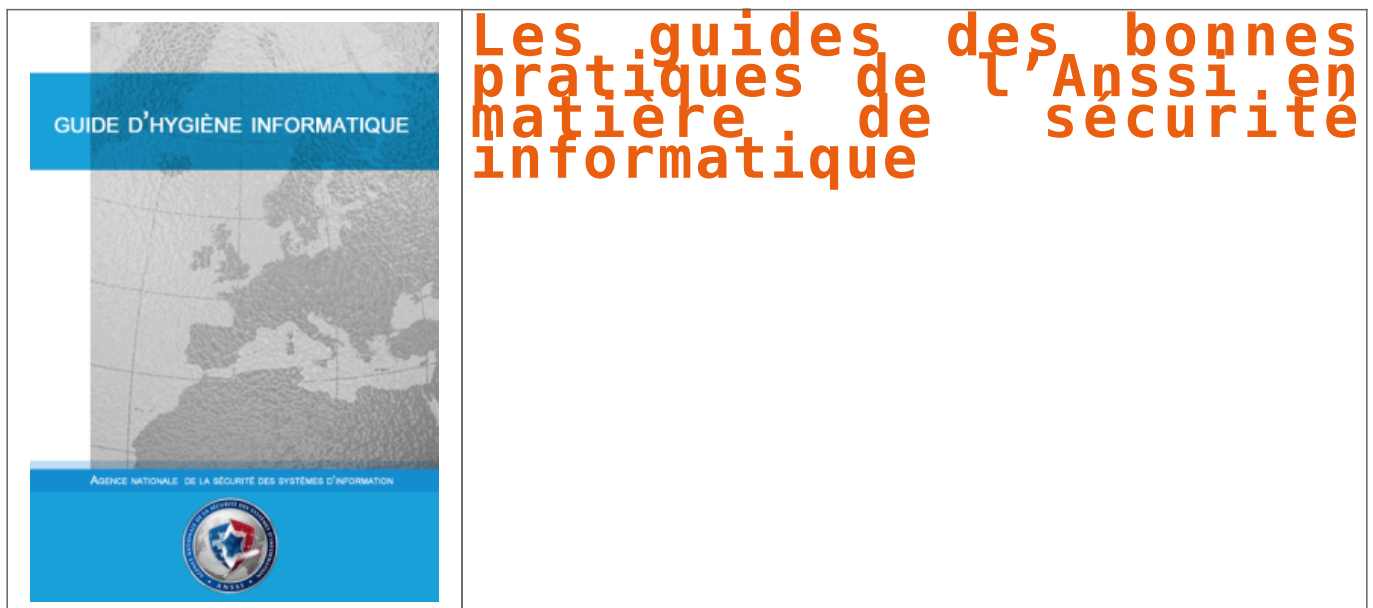
Contactez-nous

Réagissez à cet article

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

---

# Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



**Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.**

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

#### LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

---

Expert Informatique 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.ssi.gouv.fr/entreprise/bonnes-pratiques/>

---

# **RGPD Règlement européen sur la protection des données : Un renforcement des droits des personnes**



**RGPD Règlement  
européen sur la  
protection des données  
: Un renforcement des  
droits des personnes**



**Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.**

**Consentement renforcé et transparence**  
 Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.  
 L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambiguë.

**De nouveaux droits**  
 Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.  
 Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.  
 Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.  
 Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

---

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

---

À 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 (CILL) 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 93841 84)  
 Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

Denis JACOTTE est Expert Judiciaire en Informatique spécialisée en « Sécurité » et « Cybercriminalité » et en RGPD (Protection des Données à Caractères Personnelles).

**Services proposés :**

- Accompagnement à la mise en place de DPO
- **Formation** et sensibilisation à la cybersécurité et en ligne et / ou
- Audits Sécurité (ISO 27001)
- Expertise technique et juridique :
- **Incidents de sécurité** : Smartphones, Objets connectés, cartes bancaires, abonnements de services...
- **Expertise en matière de cybercriminalité**

**Le Net Expert**  
**INFORMATIQUE**  
 Spécialiste des Données Personnelles  
 Contactez-nous

Régissez à cet article

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