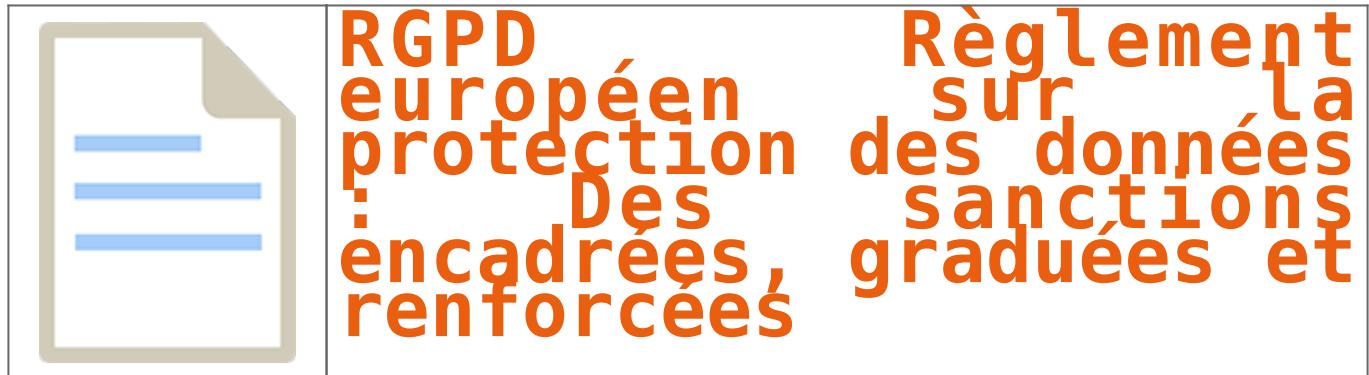


# RGPD Règlement européen sur la protection des données : Des sanctions encadrées, graduées et renforcées



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

**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 ;

# **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 cybersécurité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recyclage de preuve (téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;



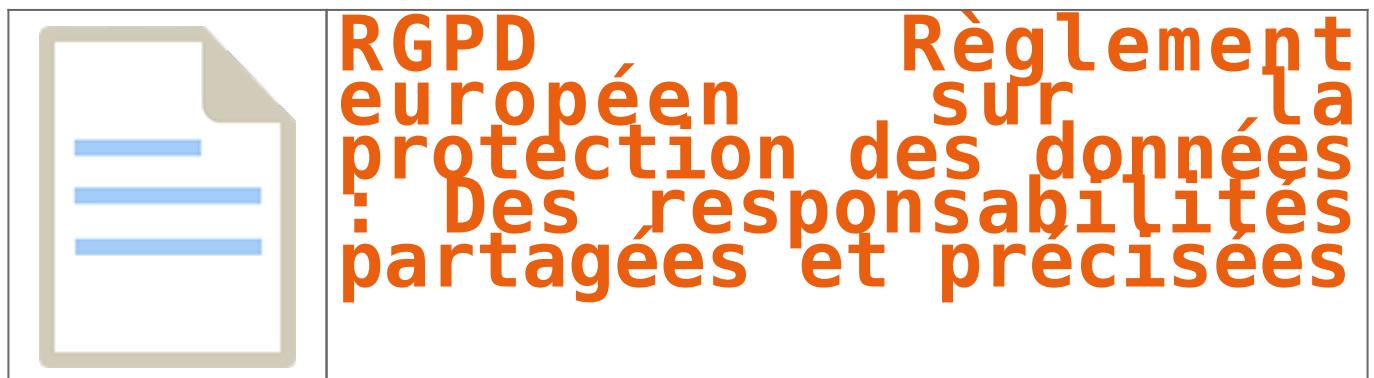
[Contactez-nous](#)

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 : 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) ;
- Expertise 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 traitée 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 amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène 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).



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

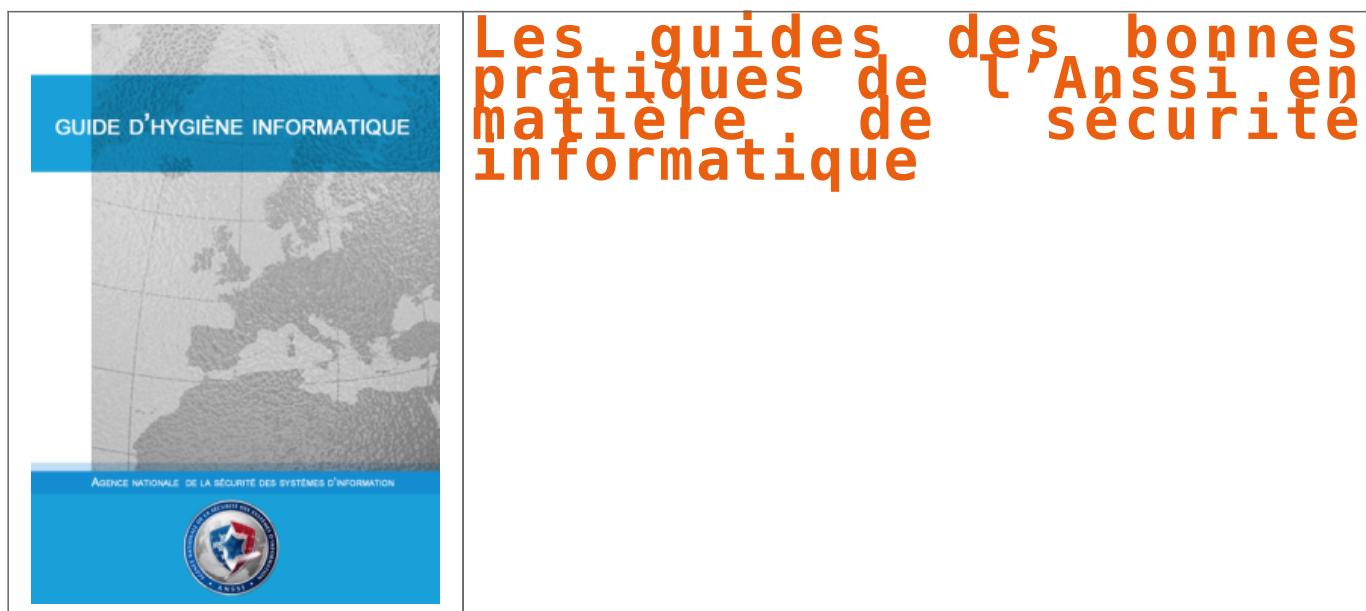
[Contactez-nous](#)

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

---

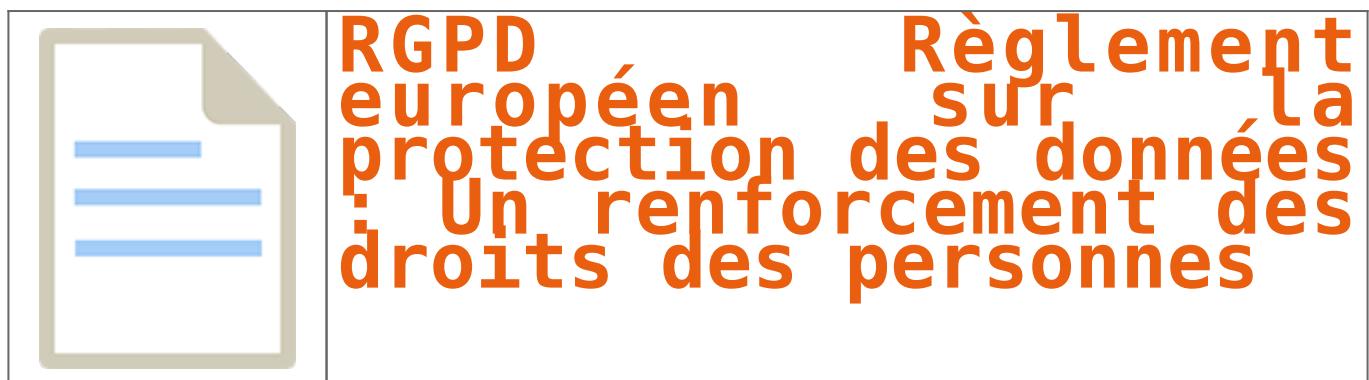
Après cette lecture, quel est votre avis ?

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**





**La Commission (Cnil) a publié, il y a peu, sa méthode pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits afin de mener des PIA (Privacy Impact Assessment).**

Dans un communiqué du 2 juillet 2015, la Commission nationale de l'informatique et des libertés (Cnil) a publiée une méthode pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits afin de mener des PIA (Privacy Impact Assessment).

Cette méthode qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la Cnil.

**Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :**

- les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés, et ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

**Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :**

- étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
- étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
- étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
- validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
  - **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.lemondedudroit.fr/droit-a-entreprises/technologies-de-linformation/208258-cnil-methode-pour-la-mise-en-conformite-et-la-prise-en-compte-de-la-vie-privee.html>

# RGPD Règlement européen sur la protection des données : Un cadre juridique unifié pour l'ensemble de l'UE



**RGPD** Règlement  
européen sur la  
protection des données  
: Un cadre juridique  
unifié pour l'ensemble  
de l'UE

**Le texte adopté est le règlement énoncé, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transcription dans les différents Etats membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.**

**Le critère de « cléage »**

Le règlement s'applique lors que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

**La responsabilité des entreprises**

Le règlement élargit la responsabilité des entreprises européennes à appliquer dans chaque pays où un résident européen sera directement visé par un traitement de données, y compris par Internet.

**La responsabilité des sous-traitants**

Le règlement étend la protection des données actuel concernant essentiellement les « responsables de traitements », à savoir les organismes qui détiennent les finalités et les modalités de traitement de données personnelles. Le règlement rend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

**Un guichet unique : le « one stop shop »**

Le règlement établit un « guichet unique » pour l'Union européenne à savoir l'autorité de protection des données de l'Etat membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficiant ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transnationaux.

**Une coopération renforcée entre autorités pour les traitements transnationaux**

Le règlement prévoit que lorsque plusieurs autorités européennes sont compétentes pour assurer la conformité des traitements de données en œuvre, les autorités de protection des données des différents Etats concernés seront juridiquement compétentes pour l'assurer sur la base de la conformité des traitements de données en œuvre.

**Attestation d'une réponse unique pour l'ensemble du territoire de l'Union**

L'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

**Procédure de contestation et de recours devant le CEPD**

En pratique, l'autorité « chef de file » proposera des mesures ou décisions (constituant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposeront alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis sera communiqué à l'autorité « chef de file » et à toutes les autres autorités concernées.

**Par exemple, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de sa demande de cohérence. Ses décisions seront définitives, susceptible de recours devant le Conseil d'Etat.**

**Par ailleurs, certaines personnes peuvent faire face à des difficultés pour se présenter régulièrement sur la conformité d'un traitement ou sur un changement au règlement et peuvent une sécurité particulière à leur entreprise et leur assurer une réponse unique sur l'ensemble du territoire de l'Union.**

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 ?

A lire aussi :

Mise en conformité RGPD : Mode d'emploi

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

Le RGPD (JO L 119 du 28 avril 2016) et le RGPD II (JO L 120 du 27 avril 2016)

Le RGPD, le règlement Européen de protection des données personnelles : RGPD ?

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)

**Autre métier : Vous accompagnez 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'audit 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).

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

Magasiner à cet article

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

# Attention aux démarchages trompeurs « Mise en conformité RGPD »

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
					
			<b>Attention aux démarchages trompeurs « Mise en conformité RGPD »</b>		

**Des courriers « Mise en conformité – RELANCE » ou « Mise en conformité – dernier rappel » avec le logo usurpé de la CNIL ou des fax « RGPD – Mise en conformité » invitent à appeler un numéro de téléphone pour ensuite facturer la fausse mise en conformité au règlement européen.**



## MISE EN CONFORMITE RELANCE

Nom du dossier :

Code contact :

Date : 19/09/2018

Objet : RGPD - Mise en conformité RGPD

Madame, Monsieur,

Nous vous rappelons qu'à compter du 25 mai 2018, les entreprises qui n'auront pas régularisé leur situation quant au nouveau règlement RGPD 2016/679 sur la protection des données, quelle que soit leur activité ou taille, sont passibles de sanctions pénales et financières pouvant s'élever jusqu'à 4% du Chiffre d'Affaire annuel de la société.

**Vous êtes invités à vous mettre en conformité sans délai.**

Le Pôle administratif RGPD a mis en place un service d'assistance téléphonique centralisé, intégralement dédié à cette circonstance, disponible du lundi au vendredi de 9h00 à 18h00 au :

- Par téléphone : (prix d'un appel local)

- En ligne : Remplir le questionnaire de pré diagnostic RGPD en ligne

Si vous avez déjà effectué votre rapport RGPD, merci de ne pas tenir compte de ce rappel.

Pôle Administratif RGPD

Le directeur régional



RAPPEL DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) - sanctions prévues

(Chapitre III, article 83, alinéa 1)

Les autorités compétentes peuvent infliger des amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou 4 % du chiffre d'affaires annuel mondial total de l'entreprise concernée, le montant le plus élevé étant retenu.

(Chapitre III, article 83, alinéa 2)

Si l'infraction est grave et récurrente ou si l'organisme en question a manifesté une volonté de nuire, l'amende peut être augmentée d'un tiers de centaine au tiers de l'infraction.

(Chapitre III, article 83, alinéa 3)

Si l'infraction est grave et récurrente, ou si l'organisme en question a manifesté une volonté de nuire, l'amende peut être augmentée d'un tiers de centaine au tiers de l'infraction.

(Modifié par la loi 2009-091 du 10 avril 2009)

La présente loi s'applique aux établissements auxquels il est fait référence, ainsi qu'aux établissements de protection des données auxquels il est fait référence. Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut l'être identifiée.

RGPD

D'après des témoignages récents, après avoir appelé au numéro indiqué sur leur document affichant fièrement une bande bleu / blanc / rouge, ils ont posé quelques questions sur l'entreprise puis envoyé par mail un facture proforma demandant de s'en acquitter sous 72h. Les escrocs vont même jusqu'à dire qu'en payant cette facture, la CNIL fera une « levée de contrôle et de sanction » sur votre société.

Puis, une fois le paiement effectué, vous aurez un entretien de 15 minutes durant lequel 50 questions vous seront posées puis sous 30 jours un « délégué syndical du département » prendra contact et clôturera définitivement la mise à jour.

**Tous ces arguments sont strictement faux !**

La mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement, par une personne qualifiée en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps. Il est nécessaire, avant tout engagement, de chercher en ligne des informations sur la société qui prend contact avec vous. Si le doute persiste, vous pouvez contacter la CNIL au 01 53 73 22 22.

**Pour vous rassurer, Denis JACOPINI et son équipe réalisent des démarches de mise en conformité des établissements avec la réglementation relative aux données à caractère Personnel depuis 2012. Plus d'informations ici**

### Nos conseils

Mettre en conformité nécessitera dans la plupart des cas une analyse de vos process, une sensibilisation du personnel, des interviews personnalisés et nous recommandons a minima une rencontre. Ces organismes ne semblent pas répondre à ces recommandations.

Au regard de pratiques commerciales trompeuses, la DGCCRF et la CNIL formulent plusieurs recommandations qui visent à :

- vérifier l'identité des entreprises démarchueuses qui ne sont en aucun cas, contrairement à ce que certaines prétendent, mandatées par les pouvoirs publics pour proposer à titre onéreux des prestations de mise en conformité au RGPD ;
- vérifier la nature des services proposés :
  - la mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement par un professionnel qualifié en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps ;
  - Dans certains cas, il peut aussi s'agir de manœuvres pour collecter des informations sur une société en vue d'une escroquerie ou d'une attaque informatique.

### Principaux réflexes à avoir en cas de démarchage

Si vous recevez ce type de sollicitations, vous devez :

- demander des informations sur l'identité de l'entreprise démarchueuse permettant de faire des vérifications sur internet ou auprès des syndicats de votre profession ;
- demander le numéro SIRET de l'organisme ;
- demander les conditions générales de vente de l'organisme ou les termes du contrat que vous devrez signer ;
- consulter le site internet et vérifier les mentions légales ;
- vérifier l'ancienneté du nom de domaine (un nom de domaine récent indique la création récente du service avec un risque de manque d'expérience ou la création d'un nom de domaine spécialement pour l'arnaque).
- vous méfier de telles communications prenant les formes d'une information officielle émanant d'un service public ;
- lire attentivement les dispositions contractuelles ou pré-contractuelles ;
- prendre le temps de la réflexion et de l'analyse de l'offre ;
- diffuser ces conseils de vigilance auprès de vos services et des personnels qui sont appelés à traiter ce type de courrier dans l'entreprise ;
- ne payer aucune somme d'argent au motif qu'elle stopperait une éventuelle action contentieuse..

Pour vous aider dans votre mise en conformité au RGPD, la CNIL publie des contenus pratiques. Vous pouvez notamment consulter « RGPD : ce qui change pour les pros » ainsi que le nouveau « Guide de sensibilisation pour les petites et moyennes entreprises » élaboré en partenariat avec la BPI.

Pour information, voici les 6 phases recommandées par la CNIL

<https://www.cnil.fr/fr/principes-cles/rgrp-se-preparer-en-6-etapes>

### et notre méthode de mise en conformité avec le RGPD :

- « Comment se mettre en conformité avec le RGPD ? »
- « Mise en conformité RGPD : Accompagnement personnalisé par un Expert »
- « Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants ».



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai 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, j'ai été ensuite Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur.

**“Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD.”**

[block id="24761" title="Pied de page HAUT"]

**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, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Vigilance : Démarchages trompeurs « Mise en conformité RGPD » | CNIL*

Illustration issue d'un témoignage

---

# Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL





Comment retirer  
des publications  
gênante sur les  
réseaux sociaux  
? Les conseils  
de la CNIL

**Sur les réseaux sociaux, vous pouvez être confronté à la diffusion d'informations personnelles publiée par d'autres internautes. Voici quelques liens utiles pour demander rapidement l'effacement de ces contenus**

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Sur une publication, vous pouvez être identifié :

- **directement** (exemple : nom, prénom, etc.)
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à votre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi votre voix ou votre image).

Votre identification peut être réalisée :

- **à partir d'une seule de vos données** (exemple : numéro de sécurité sociale, etc.)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Avant de demander la suppression du contenu, assurez-vous que le compte ou l'information n'appartient pas à un homonyme.

En cas de doute raisonnable, le réseau social peut être en mesure de vous demander tout document permettant de prouver que ce contenu vous concerne. En revanche, **il ne peut pas vous demander des pièces justificatives qui seraient abusives, non pertinentes et disproportionnées par rapport à votre demande.**

## **1. Signaler la publication à effacer**

En fonction du réseau social, vous devez vous rendre sur la page appropriée qu'il a mis à votre disposition à cet effet.

Twitter : Signaler la divulgation d'informations privées

Instagram : Signaler une photo ou vidéo pour violation de vos droits de confidentialité sur Instagram

Facebook : Utiliser le lien » Signaler »

situé à côté de la publication, de la photo ou du commentaire

Snapchat : Signaler la publication ou Utiliser ce formulaire en ligne ou Utiliser le formulaire de droit à l'image

LinkedIn : Signaler le harcèlement d'un utilisateur ou un problème de sécurité

Youtube : Réclamer une atteinte à la vie privée

Dailymotion : Sous chaque vidéo figure un bouton » Signaler cette vidéo »

en cliquant dessus, vous aurez à remplir un formulaire.

## **2. Si le réseau social ne fait pas partie de cette liste**

- Rendez-vous vous en bas de la page d'accueil du réseau social ;
- Identifiez une page « politique de confidentialité » ou « données personnelles » ou « vie privée » ;
- Dans cette page, recherchez les coordonnées du service ou le formulaire qui répondra à votre demande ;
- Envoyez si besoin un modèle à personnaliser qui comprend les références aux textes de loi et vous permet d'indiquer un motif.

**Quelle réponse attendre du réseau social ?**

Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois.

En parallèle de cette démarche d'effacement – et si ce contenu est référencé dans les moteur de recherche – exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche.

En cas de réponse insatisfaisante – ou d'absence de réponse sous un mois – de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

[block id="24761" title="Pied de page HAUT"]

## **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, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Publication gênante sur les réseaux sociaux : signalez pour supprimer ! | CNIL*