

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*

Facebook : Comment protéger ses données personnelles | Denis JACOPINI

	Facebook : Comment protéger ses données personnelles
---	--

Sur Facebook comme sur l'ensemble des réseaux sociaux, le piratage des comptes et la diffusion d'informations personnelles sont bien des problèmes très fréquents. Plusieurs fois, le réseau social a tenté de modifier sa politique de confidentialité, certes, on se pose toujours la question sur son efficacité. Quelle est donc la meilleure façon de se protéger ? Découvrez la réponse un peu plus bas...

La politique de confidentialité, toujours à craindre

Facebook prend beaucoup de la place dans notre vie quotidienne. Chaque jour, des millions de personnes se connectent sur le réseau social pour discuter et partager des photos. Facebook est même considéré aujourd'hui comme le meilleur outil de communication au quotidien comme dans la vie professionnelle. Cependant, les questions de sécurité posent toujours problème. En réalité, nombreux sont les utilisateurs de Facebook qui oublient qu'une partie de leur vie est détenue par le réseau social : leurs adresses mails, leurs numéros de téléphone, leurs lieux de travail, Bien sûr, Facebook, comme les autres réseaux sociaux, propose déjà une politique de confidentialité, certes, il arrive que les paramètres de confidentialité ne soient pas correctement ajustés. Ce qui permettrait alors à d'autres utilisateurs d'y mettre la main.

Eviter qu'une entreprise ou une organisation vous atteigne après consultation de l'onglet Publicités

Voici 2 astuces :

- Cliquez sur Verrouiller en haut à droite de votre page Facebook, puis sur Paramètres.
- Aller sur Modifier dans la première partie intitulée : Sites tiers. Vous pourriez ainsi modifier vos paramètres en remplaçant Mes amis uniquement par Personne, puis en enregistrant ces nouvelles modifications.

Prenez garde des publicités sociales

Vous pouvez également vous protéger de la publicité sociale et de l'exploitation de données par les applications partenaires de Facebook en passant par ces quelques étapes :

- Dans paramètre, cliquer sur l'onglet Applications qui se trouve dans la colonne de gauche. Vous découvrirez ainsi une liste complète d'applications
 - Cliquer sur chacune d'entre elles, supprimez-les ou encore consulter les informations qui vous concernent personnellement
 - En cliquant sur le crayon, vous pourriez vous apercevoir que l'application en question connaît votre prénom, votre tranche d'âge, votre adresse mail, mais surtout ne paniquez pas. Il vous suffit de fermer cette fenêtre et d'aller plus bas sur la page des Applications. Vous pouvez toujours modifier les paramètres de façon à ce qu'elles se jouent anonymement.

Malheureusement, supprimer ses photos ne suffit pas à se protéger. D'ailleurs, il est impossible de savoir si une photo est réellement supprimée du serveur Facebook.

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 plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.infos-mobiles.com/facebook/facebook-comment-proteger-ses-donnees-personnelles/102992>

Par HA75

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

	<p>RGPD Règlement européen sur la protection des données Le cadre des transferts hors de l'Union mis à jour</p>
---	---

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

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 ;**

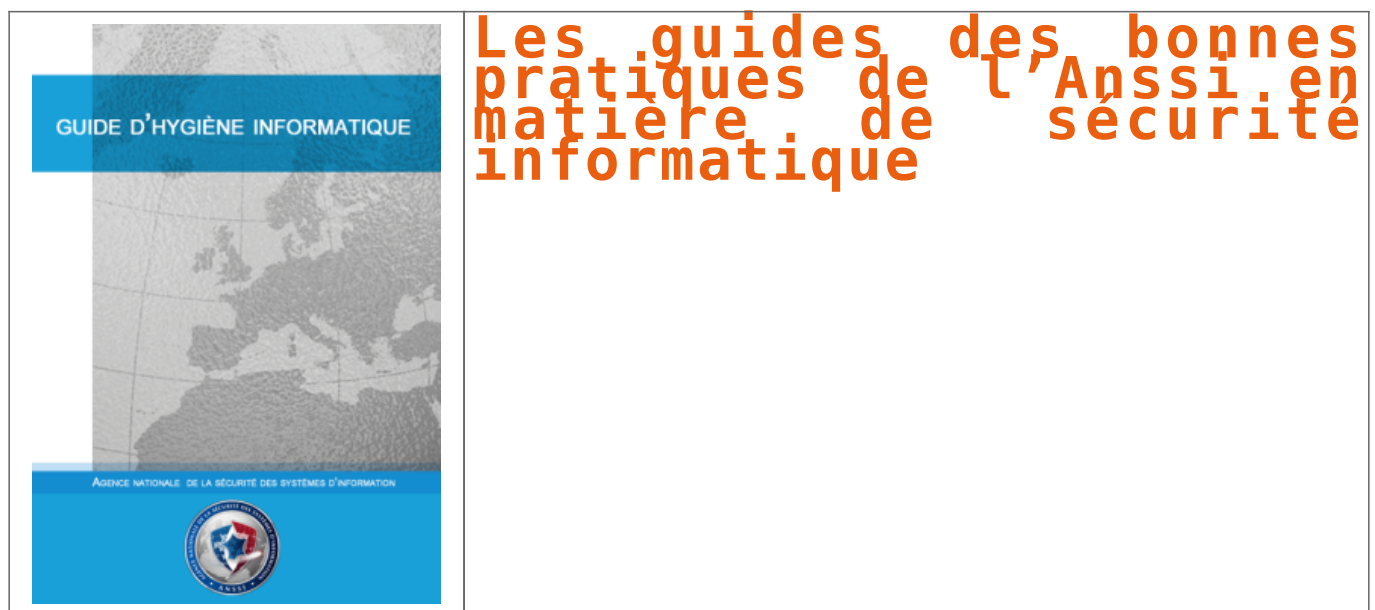


[Contactez-nous](#)

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**

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

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 Responsable 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

Deux JACOPHE en Expert Sécurité en Informatique spécialisé en « Sécurité et Cybersécurité » et en RGPD (Protection des Données à Caractère Personnel).

- **Responsable Informatique et Libertés (CIL)**
- **Accompagnement à la mise en place de DPO :**
- **Formation** (et sensibilisation) à la « Sécurité et Cybersécurité » (pour tous les usagers) ;
- **Audits Sécurité (ISO 27001) :**
- **Expertise** (sur les risques) : vulnérabilités, risques
- **Plan d'action** : cybersécurité, accompagnement de clientèle

Vous souhaitez en savoir plus sur nos services ?


 **Le Net Expert**
INFORMATIQUE
Consultant en Cybersécurité et Sécurité des Données

Contactez-nous

Régistrez à cet article

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


Cnil : méthode pour la mise en conformité et la prise en compte de la vie privée | Le Net Expert Informatique



Le Net Expert

INFORMATIQUE

Protection des données personnelles
Sécurité Informatique - Cybercriminalité



vous informe...

Cnil : méthode pour la mise en conformité et la prise en compte de la vie privée

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 plait ? 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



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

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

Attention aux démarchages trompeurs « Mise en conformité RGPD »

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

Numéro de dossier :
Code client :
Date : 19/09/2018
Objet : 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 pécuniaires et financières pouvant s'élever jusqu'à 4% du Chiffre d'Affaire annuel de la société.

Vous des incités à vous mettre en conformité avec le RGPD.

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 09h00 à 18h00 au :

- Par téléphone : (01 53 73 22 22) (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



ARTICLE DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions pécuniaires
(Changement 100 article 83, alinéa 2)
Les violations des dispositions suivantes font l'objet d'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.
Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions civiles
(Changement 100 article 82, alinéa 2)
Sans préjudice de tout recours administratif ou judiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'un organe de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif et adéquat en raison des dommages matériels ou moraux qu'elle a subis.
La présente loi a pour objet de transposer en droit français le règlement européen relatif à la protection des données à caractère personnel (RGPD) et de compléter ce dernier.
La loi n° 78-17 du janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Loi Informatique et Libertés) est modifiée.
La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou relatives à figure dans des fichiers. Contraire une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée.

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 à minimas 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 démarcheurs 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 démarcheuse 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/rgpd-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