

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-protoger-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

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*

Compte Facebook piraté : Quelles sont les bons réflexes à avoir ? | Denis JACOPINI

21



Compte Facebook piraté :
Quelles sont les bons
réflexes à avoir ?

Il arrive parfois de se faire pirater son compte Facebook. Soit parce qu'on a oublié de se déconnecter du site sur un ordinateur public, soit parce qu'on s'est fait voler d'une manière ou d'une autre son mot de passe. Il arrive aussi que des personnes se fassent passer pour vous et ouvrent un profil à votre nom avec vos informations et photos personnelles.

Dans ces cas de piratage ou d'usurpation d'identité, il importe de réagir rapidement pour empêcher toute possibilité de nuisance.
Première chose à faire : signaler le compte piraté ou usurpé à Facebook.

Si votre compte a été piraté

Signaler un compte piraté

Si vous pensez que votre compte a été piraté ou infecté par un virus, cliquez sur le bouton Mon compte a été piraté ci-dessous. Nous vous aiderons à vous reconnecter afin d'en reprendre le contrôle.

Mon compte a été piraté

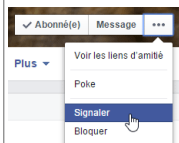
Annuler

Rendez-vous sur la page Signaler un compte piraté.

Indiquez l'identifiant de votre compte puis suivez les instructions. Vous serez notamment amené à taper votre ancien mot de passe et Facebook vous posera quelques questions pour vérifier votre identité.
Dans le pire des cas, vous pourrez faire appel à contacts de confiance pour récupérer votre compte.

Si votre identité (ou celle d'une autre personne) a été usurpée

Rendez-vous sur la page du profil suspicieux et cliquez sur le bouton contenant 3 petits points, juste en dessous de la photo de couverture. Sélectionnez Signaler.



Dans la fenêtre qui s'affiche alors, sélectionnez l'option Signaler ce compte et cliquez sur Continuer.

Aidez-nous à comprendre ce qui se passe

Que voulez-vous faire ?

☐ Signaler du contenu partagé par Gauthier

☒ Signaler ce compte

☐ Obtenir de l'aide pour un autre problème

Continuer

Dans l'écran suivant, sélectionnez ensuite l'option Ce journal se fait passer pour quelqu'un que je connais.

Aidez-nous à comprendre ce qui se passe

Quel est le problème avec ce compte ?

☐ Cette personne me dérange

☒ Ce journal se fait passer pour moi ou quelqu'un que je connais

☐ Ce journal contient beaucoup de contenus inappropriés

☐ C'est un compte frauduleux

☐ Ce profil représente une entreprise ou une organisation

☐ Ce journal utilise un faux nom

Retour

Continuer

Vous êtes amené ensuite à préciser votre cas.

Aidez-nous à comprendre ce qui se passe

Qui prétendent-ils être ?

☒ Moi

☐ Une personne que je connais

☐ Une célébrité

Retour

Continuer

S'il s'agit de votre propre identité, sélectionnez l'option Moi. Vous pouvez alors demander à fermer le compte.

Si l'identité de quelqu'un d'autre a été usurpée, sélectionnez l'option Une personne que je connais ou éventuellement Une célébrité.
Cliquez sur Continuer pour valider et suivez les instructions.

Aller plus loin et porter plainte

Si vous estimez qu'il y a préjudice, vous pouvez aller porter plainte au Commissariat de police ou à la Gendarmerie de votre lieu d'habitation. N'hésitez pas à faire des captures d'écran pour nourrir votre dossier.

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

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

Source : <http://www.aussitot.fr/facebook/signaler-compte-pirate-usurpation-identite-facebook.html>

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 ;**

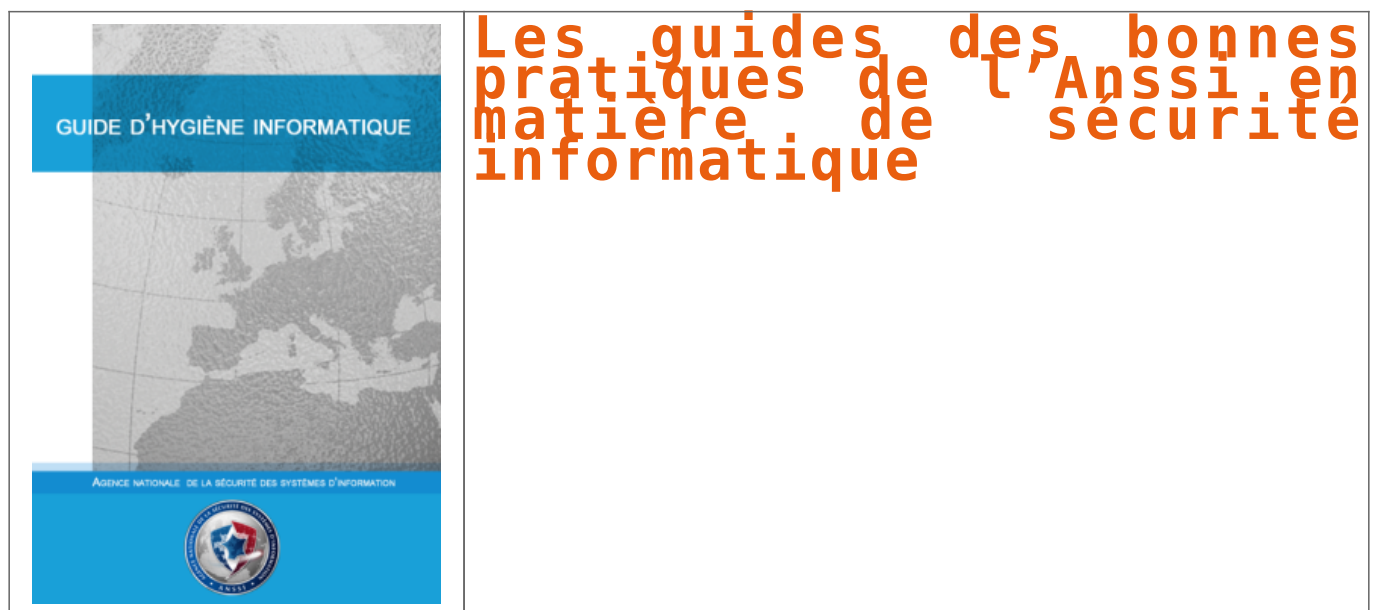


[Contactez-nous](#)

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.

[Retourner à la page précédente](#)

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

Denis JACOBINE est Expert technique en informatique spécialisée 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
- **Sensibiliser** et contribuer à la culture de la sécurité des données au sein de l'entreprise
- Audits Sécurité (ISO 27001)
- Expertise des risques liés aux données
- Gestion des incidents, violations, demandes de confidentialité

[Retourner à la page précédente](#)

Le Net Expert
INFORMATIQUE
Consulting et Cyberprotection

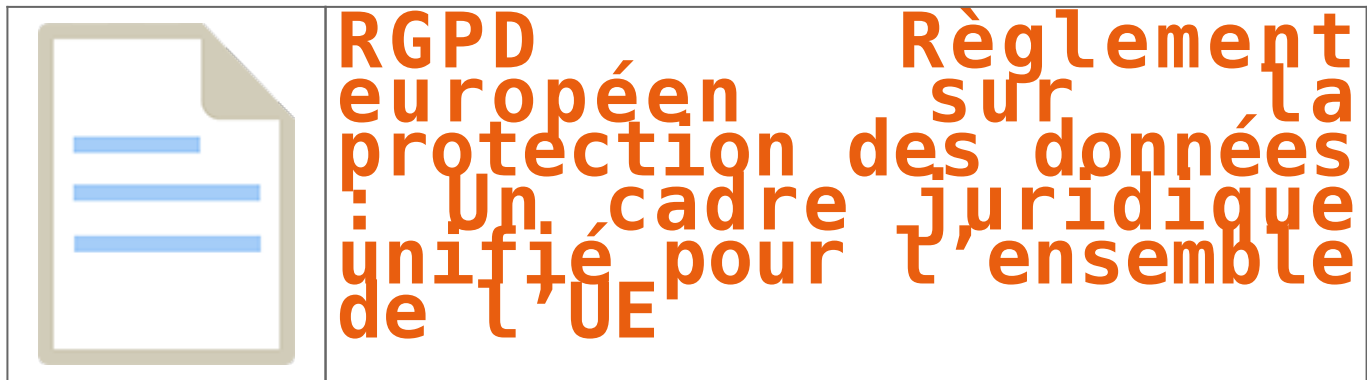
Contactez-nous

[Retourner à la page précédente](#)

Régistrez 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 : Un cadre juridique unifié pour l'ensemble de l'UE



Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le site texte s'applique 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.

Un champ d'application étendu
Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou 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).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

La responsabilité des sous-traitants
Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitement », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »
Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désigné 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 de traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettent en œuvre des traitements transnationaux.

Une coopération renforcée entre autorités pour les traitements transnationaux
Toutefois, dès lors qu'un traitement sera transnational – quel qu'il concerne les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernés seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer 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 conjuguées. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'Article 28 du préambule. L'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent 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. Ce avis est contraignant et doit être suivi par l'autorité « chef de file ».

Si le CEPD suit ou non l'avis, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjuguée, susceptible de recourir devant le juge des décisions de l'autorité « chef de file ».

Par exemple, dans le cas d'une entreprise qui s'établit principalement en France, la CNIL sera le guichet unique de cette entreprise et lui soumettra les décisions adoptées dans le cadre de sa mise en œuvre de conformité. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recourir devant le Conseil d'État.

Le mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un engagement au règlement et garantit une autorité juridique élevée aux entreprises en leur assurant 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 ?
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
Règlement (UE) 2016/679 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'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 Liberté (CIL) ou d'un Délégué à la Protection des Données (DPO) dans votre établissement, l'habilitation de la Direction de Travail de l'Usager et de la Fonction Professionnelle (DTPU) ou d'un Délégué à la Protection des Données (DPO).
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement européen pour la Protection des Données Personnelles

Vous souhaitez en savoir plus sur nos services et nos tarifs ?
Contactez-nous

Le Net Expert
INFORMATIQUE
Contactez-nous

Régistrez à cet article

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

Les métiers de la cybersécurité en 2020

LE NET EXPERT
AUDITS & EXPERTISES

LE NET EXPERT
EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES
LENETEXPERT.fr

LE NET EXPERT
MISES EN CONFORMITÉ

SPY DETECTION
Services de détection de logiciels espions

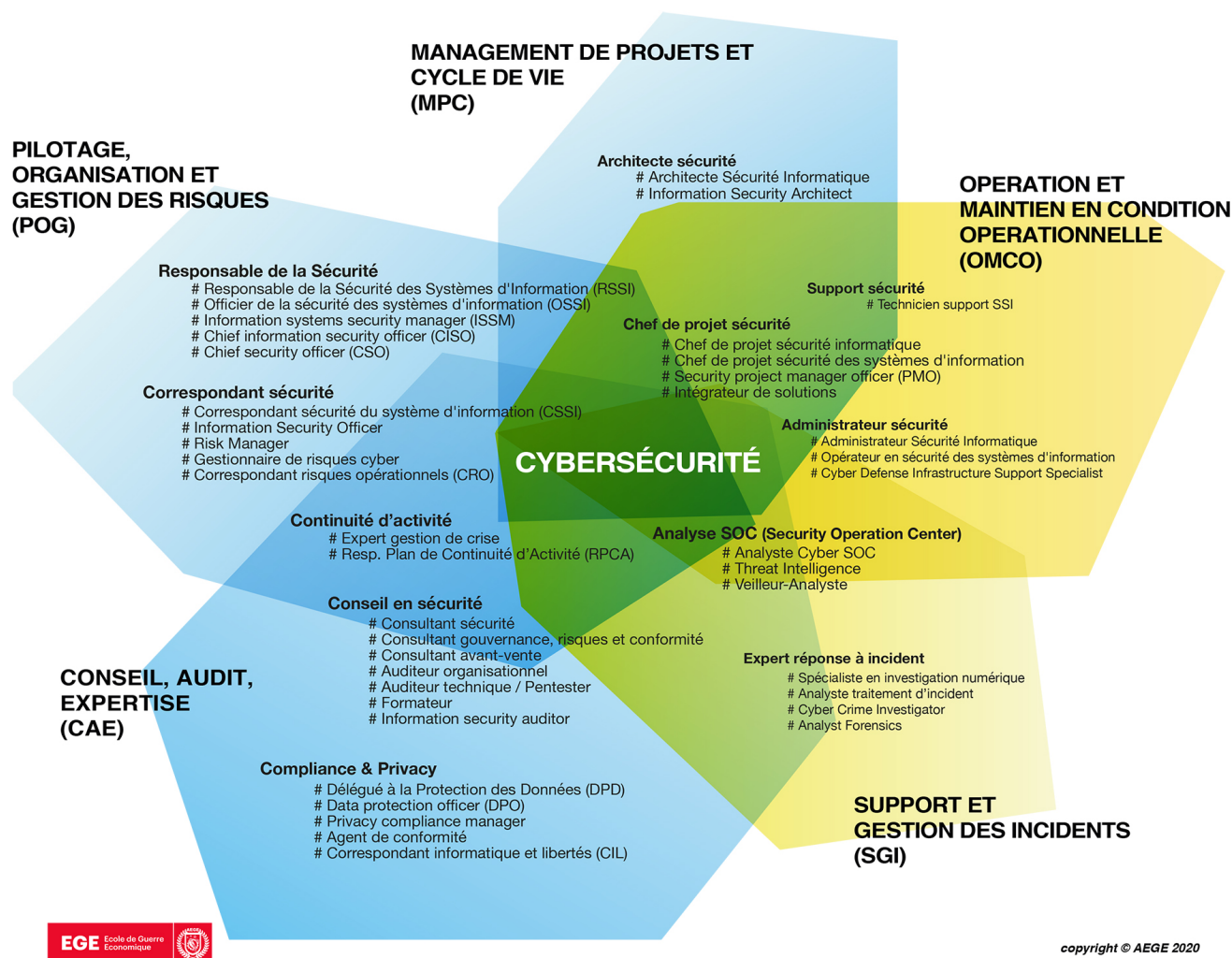
LE NET EXPERT
FORMATIONS

LE NET EXPERT
ARNAQUES & PIRATAGES

Denis JACOPINI
vous informe

Les métiers de la cybersécurité en 2020

L'Ecole de Guerre Economique et le Club Cyber de l'AEGE publient la « Cartographie des métiers de la Cybersécurité » dans le cadre des formations dispensées à l'Ecole depuis 2016. Les zones bleues se rapportent à des familles de métiers Cyber typés management, alors que celles en jaune sont plus orientés ingénierie et technique.



[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 : *L'Ecole de Guerre Economique publie la cartographie des métiers de la cybersécurité 2020 | Ecole de Guerre Economique*