Le cadre légal de la géolocalisation des salariés | Denis JACOPINI

Le cadre légal de la #géolocalisation des salariés

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

1. Que le dispositif soit mis en œuvre par l'entreprise ou par l'intermédiaire d'un prestataire, c'est à l'employeur que revient l'obligation de procéder à la déclaration auprès de la Commission nationale informatique et libertés (Cnil).

2. Cette déclaration doit notamment exposer les raisons et les objectifs auxquels répond le dispositif permettant la localisation des employés (lutte contre le vol, gestion des temps de parcours, par exemple). L'employeur doit nécessairement attendre le récépissé de déclaration délivré par la Cnil pour mettre en action son dispositif.

3. Selon les exigences de la Cnil, le traitement d'informations relatives aux employés doit être proportionné à la finalité déclarée, c'est-à-dire qu'il doit s'effectuer de façon adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi.

4. L'employeur doit informer ses employés (par courrier ou réunion d'information) de la mise en œuvre du dispositif de géolocalisation et des informations qui vont être collectées. À défaut, il s'expose à une amende de 1 500 euros. L'information doit porter sur l'identité et l'adresse du responsable du traitement, la ou les finalités du traitement, les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement, les destinataires de ces données (direction, services RH ou comptables), l'existence d'un droit d'accès et de rectification et d'opposition et leurs modalités d'exercice.

5. La non-déclaration de traitement à la Cnil par la société est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende.

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

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

RGPD Règlement européen sur la protection des données : Où trouver le texte ?

RGPD Règlement européen sur la protection des données : Où trouver le texte ?

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

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

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

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

RGPD Règlement européen sur la 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 ;

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*

Facebook : Comment protéger ses données personnelles | Denis JACOPINI

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 sécurités posent toujours problème. En réalité, nombreux sont les utilisateurs de Facebook qui oublient qu'une partie de leur vie sont détenus 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 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

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

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

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

Par ailleurs, les données transférées hors Union restent soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.
Ainsi, et hormis les transferts fondés sur une décision d'adéquation de la Commission Européenne, les responsables de traitement et les sous-traitants peuvent mettre en place :
• des règles d'entreprises contraignantes (BCR) ;
• des clauses contractuelles types approuvées par la Commission Européenne ;
• des clauses contractuelles adoptées par une autorité et approuvées par la Commission européenne.

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

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

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

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

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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*

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 ;

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*

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).

- 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 ;

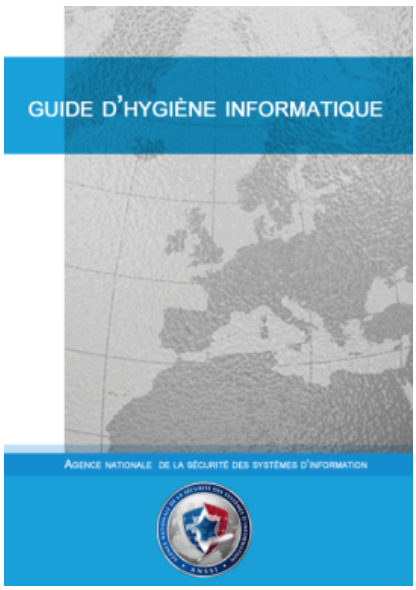
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

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



Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique

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

---

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

Source : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

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

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

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

Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

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 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

---

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*

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

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 publée 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.

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