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



Contactez-nous

Réagissez à cet article

## 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). DPO; de sessibilisations of controlled (et sessibilisations) ophocraminalité (ulteration n'els) (albertain n'els) (alber | Le Net Expert

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

### RGPD Règlement européen sur

## la protection des données : Des responsabilités partagées et précisées



Le règlement européen sur la protection des données vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations pesant sur les responsables de traitements et les sous-traitants. Le représentant légal C'est le point de contact de l'autorité. Il a mandat pour « être consulté en complément ou à la place du responsables de traitement sur toutes les questions relatives aux traitements » le sous-traitant Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability. Il a notamment une obligation de conseil auprès du responsables de traitement pour la conformité à certaines obligations du règlement (PIA, failles, sécurité, destruction des données, contribution aux audits) Il est tenu de maintenir un registre et de désigner un DPO dans les mêmes conditions qu'un responsable de traitement. Besoin d'un accompagnement pour vous mettre en conformité avec le RGPD ? ? Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ? Contactez-nous A Lire aussi : Mise en conformité RGPD : Mode d'emploi Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 Le RGPD, règlement européen de protection des données. Comment devenir DPO ? Comprendre le Règlement Européen sur les données personnelles en 6 étapes Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à 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 Accompagnement à la mise en place de DPO;



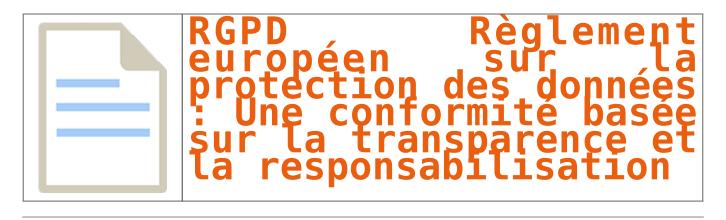


Contactez-nous

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



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 ?

A Lire aussi :

Contactez-nous

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 ravail 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).

\*\*Misse en conformité (RGQ):

\*\*Accompagnement à la mise en place de DPO;

\*\*Formations\*\* (et sensibilisations) à la cybercriminalité (autorisation n°93 84 0941 84);

\*\*Audits Sécurité (ISO 270005):

\*\*Expertises techniques et judiciaires ;

\*\*Recherche de prouve téléphones, disques de clientèle...;

\*\*Expertises techniques de fudiciaires;

\*\*Recherche de prouve téléphones, disques de clientèle...;

\*\*Expertises techniques et judiciaires;

\*\*Recherche de prouve téléphones, disques de clientèle...;

\*\*Expertises techniques et judiciaires;

\*\*Recherche de prouve téléphones, disques de clientèle...;

\*\*Paraction des la contentie (RGQ)

\*\*Recherche de prouve téléphones, disques de clientèle...;



Contactez-nous

Réagissez à cet article

## 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 domnées 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 traitement	
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 inférieu	r à 13 ans. Devenu adulte, le consentement donné sur un traitement doit
pouvoir être retiré et les données effacées.	
Introduction du principe des ections collectives: Tout comme pour la législation relative à la protection des consomnateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en mu recours collectivis en matière de protection des domnées personnelles.	stière de protection des données auront la possibilité d'introduire des
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 répu	ration du préjudice subi.
Besoin d'un accompagnement pour vous mettre en conformité avec le RGPO ? ?	
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	
Reglement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016	
DIRECTIVE (UE) 2016/698 DU PARLEMENT EUROPEEN ET DU CONSELL du 27 avril 2016	
Le RGPD, realement européen de protection des données. Comment devenir PPD ?	
Comprendre le Règlement Européen sur les données personnelles en 6 étapes	
Comprendre Le Registerent curiopemi sur les ouniers personnectes en o etapes.  Notre sélection d'articles sur le RGPD (Rèalement Européen sur la Protection des données Personnelles) et les DPD (Déléaués à la Protection des Données)	
Motre selection d'articles sur le NGPD (Reglement Europeen sur la Protection des données) et les DPD (Delegues à la Protection des Données)	
Notre métier : Yous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des domnées 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	
personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPD) dans votre établissement. (Autorisation de la Direction du travail de l'Emploi et c	le 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 JACOPPR est Deport Judokine en Informatique spécialisé en « Sécurité »	
« Cybercrinisoldié » et no RGPD (Potostatos des Données à Conselére Personnel).	
*Accompagnment à la mise en place de	
DOO;	
OCTUDE (I sentimente) II III  OCTUDE (I sentimente) II II  OCTUDE (I sentimente) II	
Audits Skombi (80 2005);	
Expertises tabularises et judiciaries;     New York Control of the Control o	
Does ACCIPIN dury, e-mails, contentious, détoumements	
o cleritie .:	
The state of the s	
- Lo Not Evport	
C   re wer exhert	
↑ INFORMATIQUE Consideration	
Southward to the Control of the Cont	
Réagissez à cet article	

## 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 direct dissonitions du réplement.	tement applicable dann l'ensemble de l'Union sams nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dann toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, lu	les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les
Un champ d'application étendu		
	titire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en moure des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anolisis monitor).	
En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé p	mar 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 « responsai	bles de traitements », 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 responsab	oles de traitement.
Un guichet unique : le « one stop shop »	ss de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur sièce central dans l'Union, soit l'établissement au sein duquel seront s	
bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données pa		prises les decisions relatives aux finalités et aux modalités ou traitement. Les entreprises
Une coopération renforcée entre autorités pour les traitements transnation		
Afin d'assurer une réconse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coco-	erra avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.	
	ms (CEPO), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G20.	
	aitement 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. Cet
avis est contraignant et doit donc être suivi par l'autorité « chef de file ».		
	gues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».	
	that unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohèmence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devent le Conseil d'État.  Ité d'un traitement ou sur un manuement sur relacement et oursett une sécurité une sécurité une sécurité unificue élemès aux entreprises en leur assurant sur enfonces unique sur l'ensemble du territoire de l'Union.	
te mecanisme permet ainsi aux autorites de protection des données de se protoncer rapidement sur la conformi	te d'un traitement ou sur un manquement au regiement et garantit une securite juricoque eux entreprises en Leur assurant une reponse unique sur l'ensemble du territoire de l'Union.	
Descin d'un accompagnement pour vous mettre en conformité avec le REFD 7 ?		
Besoin d'une formation pour apprendre à vous		
mettre en conformité avec le RGPD ?		
Contactez-nous		
· ·		
A Lire wasi :		
Mise en conformité RGPO : Node d'emploi		
Formation RGPD : L'essentiel sur le réplement Européen pour la Protection des Données Personnelles		
Réglement (UE) 2016/679 du Parlement européen et du Conneil du 27 avril 2016		
DIRECTIVE (NE) 2016/600 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 myril 2016		
Le RGPD, règlement européen de protection des données. Comment devenir DPG 7		
Comprendre le Règlement Européen sur les données personnelles en 6 étapes		
Notre sélection d'articles sur le RGPO (Règlement Européen sur la Protection des données Personnelles) et le	m DPO (Délégués à la Protection des Données)	
Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réplementation relative à l		
	a protection ons domines a caractere personni.  operation ons domines a caractere personni.  operation ons domines a caractere personni.  operation and the second operation of the caractere personnic (PSPD) on vous assistant data the caractere personnic operation of the caractere personnic (PSPD) on vous assistant data the caractere personnic operation of the caracteristic operation operation operation of the caracteristic operation operation operati	to stor or store dies formeredest federations at Libertia (CEL) on dies flots flootester
Officer (DPO) dans votre établissement (Autorisation de la Direction du travail de l'Emploi et de la Forma'		in ta mile en place o un correspondant innomacique et cibertes (cib) ou o un osca Procection
Plus d'informations sur : Formation RGPO : L'essentiel sur le règlement Européen pour la Protection des Donn	eles Personnelles	
Desis SKOPINI est Esperi Auktore en Informétique spéciales en « tricurtoi » « Cubecommitté » et en ROPO Protection des Données à Considére Responsif.		
• Mose an architecture (in the control of the contr		
- Parallelle pe someognet & Mr		
Auto Situati (50 2009);		
Dispersion to Delegate of Justices ;     Delegate of Justices delegate of Justices ;		
the Access day, e-mile, contribut, deburements		
Contract of waters of waters of contract of the contract of th		
- Le Net Expert		
- INFORMATIQUE CONSUMENT		
Company of Company Proceedings		
H		

## 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.



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 a jour.

Tous ces arguments sont strictement faux !

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

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

#### Nos conseils

Mettre en conformité nécessitera dans la plupart des cas une analyse de vos process, une sensibilisation du personnel, des interviews personnalisés et nous recommandons a 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 démarcheuses 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."

## 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

## Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI



Votre responsabilité engagée en cas de piratage de vos données





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



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

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

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

Votre identification peut être réalisée :

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

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

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

1. Signaler la publication à effacer

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

Twitter : Signaler la divulgation d'informations privées

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

Facebook : Utiliser le lien » Signaler «

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

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

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

Youtube : Réclamer une atteinte à la vie privée

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

en cliquant dessus, vous aurez à remplir un formulaire.

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

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

#### Quelle réponse attendre du réseau social ?

Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois. En parallèle de cette démarche d'effacement — et si ce contenu est référencé dans les moteur de recherche — exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche. En cas de réponse insatisfaisante — ou d'absence de réponse sous un mois — de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

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

## Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

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

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

## Nos ordinateurs ont-ils la mémoire courte ? Vidéo



Nos. ordinateurs ont-ils la mémoire courte ? Vidéo Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore. Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[lire la suite]

#### LE NET EXPERT

:

- MISE EN CONFORMITÉ RGPD / CNIL
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
  - MISE EN CONFORMITÉ RGPD de vos traitements
    - **SUIVI** de l'évolution de vos traitements
      - FORMATIONS / SENSIBILISATION :
        - CYBERCRIMINALITÉ
      - PROTECTION DES DONNÉES PERSONNELLES
        - AU RGPD
        - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
    - SYSTÈMES NUMÉRIQUES
  - EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - **SÉCURITÉ** INFORMATIQUE
    - SYSTÈMES DE VOTES ÉLECTRONIQUES

#### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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



- 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

×

Source : Nos ordinateurs ont-ils la mémoire courte ?