

Vers une nouvelle loi relative à la protection des données personnelles



Le projet de loi déposé à l'Assemblée nationale vise la réalisation en droit français du paquet protection des données personnelles de l'Union européenne au 25 mai 2018. Les délais sont courts pour les acteurs qui doivent se conformer à un texte dont la lisibilité est complexe.

Par Olivia TambouLe nouveau projet de loi français relatif à la protection des données personnelles était attendu. Il permet de concrétiser en droit français la réforme du droit européen de la protection des données personnelles adoptée en avril 2016¹. L'ambition affichée est d'adapter ce droit aux évolutions technologiques en facilitant la libre circulation des données personnelles tout en assurant un niveau de protection élevé des individus. Cette harmonisation opère un changement de paradigme à l'échelle de l'Union européenne. Elle propose un renforcement de la régulation par les responsables de traitement, leurs sous-traitants et les autorités de la protection des données sous le contrôle des juges. L'objectif est d'inculquer aux acteurs une véritable culture de la protection des données personnelles prise en compte dès la conception de leurs produits et services, et dans leur organisation interne. Il suffit ici d'évoquer la nécessité de pouvoir documenter le respect de ses obligations, de procéder à une analyse d'impact préalable ou encore l'obligation de désigner un délégué de la protection des données personnelles (DPO) pour certains traitements aux risques élevés au regard des droits et libertés des individus....[lire la suite]

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 DRTF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *Vers une nouvelle loi relative à la protection des données personnelles – Atteinte à la personne | Dalloz Actualité*

Carphone Warehouse condamné à une amende de 500 000 par la CNIL équivalente au Royaume-Uni



L'organisme de surveillance des données du Royaume-Uni a infligé une amende de 400 000 £ à l'opérateur de téléphonie mobile Carphone Warehouse, soit un peu moins que les 500 000 £ actuellement accordés par l'organisme de réglementation.

Les données client compressées comprenaient: les noms, adresses, numéros de téléphone, dates de naissance, état civil et, pour plus de 18 000 clients, les détails historiques des cartes de paiement. Tandis que les dossiers exposés pour certains employés de Carphone Warehouse, y compris le nom, les numéros de téléphone, le code postal, et les détails d'immatriculation de voiture. Commentant la pénalité dans un communiqué, Elizabeth Denham, commissaire britannique à l'information, a déclaré: «Une entreprise aussi grande, bien dotée en ressources et établie que Carphone Warehouse, aurait dû évaluer activement ses systèmes de sécurité des données et s'assurer que les systèmes étaient robustes et non vulnérables. à de telles attaques.

« Carphone Warehouse devrait être au sommet de son jeu en matière de cybersécurité, et il est inquiétant de constater que les échecs systémiques que nous avons relevés sont liés à des mesures rudimentaires et banales. »

Le Bureau du Commissaire à l'information a déclaré avoir identifié de multiples insuffisances dans l'approche de la société en matière de sécurité des données au cours de son enquête et a déterminé que la société n'avait pas pris de mesures adéquates pour protéger les informations personnelles.

Les intrus ont été en mesure d'utiliser des informations d'identification valides pour accéder au système de Carphone Warehouse via un logiciel WordPress obsolète, a indiqué l'ICO.

Les insuffisances dans les mesures techniques de sécurité de l'organisation ont également été mises en évidence par l'incident, les éléments importants du logiciel utilisé sur les systèmes affectés étant obsolètes et l'entreprise ne procédant pas aux tests de sécurité de routine.

Il y avait aussi des mesures inadéquates en place pour identifier et purger les données historiques, a-t-il ajouté.

« Il y aura toujours des tentatives pour briser les systèmes des organisations et les cyber-attaques deviennent plus fréquentes à mesure que les adversaires deviennent plus déterminés. Mais les entreprises et les organismes publics doivent prendre des mesures sérieuses pour protéger les systèmes, et surtout, les clients et les employés », a déclaré Denham.

« La loi dit qu'il est de la responsabilité de l'entreprise de protéger les informations personnelles des clients et des employés. Les étrangers ne devraient pas avoir accès à de tels systèmes en premier lieu. Avoir un système de sécurité en couches efficace aidera à atténuer toute attaque – les systèmes ne peuvent pas être exploités si les intrus ne peuvent pas entrer. »
« ..[lire la suite]

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.



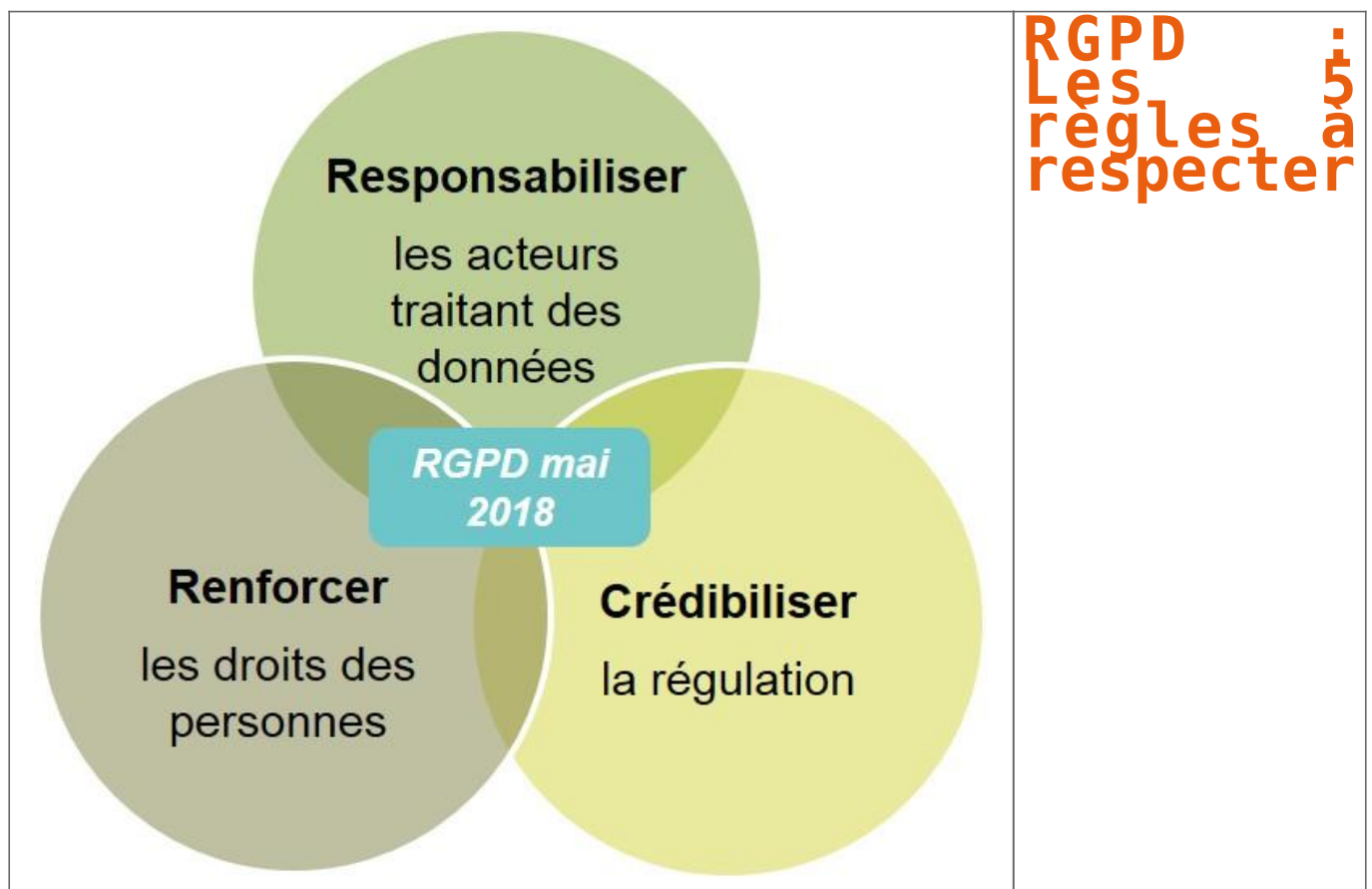
[Contactez-nous](#)



Réagissez à cet article

Source : *Le Carphone Warehouse du Royaume-Uni condamné à une amende de 540 000 \$ pour piratage de 2015*

RGPD : Les 5 règles à respecter



A partir du 25 mai 2018, toutes les entreprises gérant et collectant des données sur les personnes devront respecter chacune des obligations du Règlement européen pour la protection des données, le RGPD. Toutes les entreprises sont donc concernées par ce règlement que vous fassiez de l'outbound ou de l'inbound marketing. Le règlement prévoit également de lourdes sanctions en cas de violation de clauses : votre entreprise est-elle prête ?

Avez-vous préparé votre entreprise aux nouvelles normes de protection des données ? Faisons le point sur les 5 règles majeures à respecter.

- La protection réelle des données, le principe du Privacy by design
- Le consentement du consommateur
- Le vrai droit à l'oubli ou « droit à l'effacement »
- L'accès de l'utilisateur à ses données
- Le délégué à la protection des données – DPO

En amont même de la réalisation du projet, dès les premières étapes de sa conception, la protection des données personnelles devra s'imposer comme une exigence, dans le cahier des charges. C'est le principe du **Privacy by design**, soit la protection dès la conception du projet, du service, du produit ou du système. Corrélativement, la règle de la sécurité par défaut devra être appliquée : toute entreprise concernée devra disposer d'un système sécurisé.

Il est obligatoire de demander et d'obtenir le **consentement du consommateur** pour collecter ses données. Il est obligatoire de faire cocher la case, et il est interdit d'utiliser une case – ou autre dispositif – autorisant par défaut la collecte (exemple : case déjà cochée).

Dès lors qu'un individu en fait la demande, tous les acteurs concernés par le RGPD auront un délai de 30 jours pour **supprimer ses données**.

De la même manière, il est obligatoire pour le responsable des données de notifier ce droit, ainsi que le droit à la limitation dans l'utilisation des données et le droit de rectification des données. L'utilisateur a le **droit d'accès** permanent, et de contrôle sur ses propres données.



Nommé au sein de l'entreprise, le **DPO** (pour rappel le délégué à la protection des données) doit mettre en œuvre 3 principes :

1. Privacy by design
2. le Privacy by default, par lequel le plus haut niveau de protection est assuré
3. l'Accountability, soit la transparence et la démonstration de sa parfaite conformité devant les autorités.

[lire la suite]



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 ».

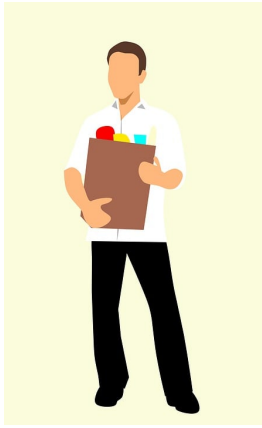
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contenu, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (souvent en direct en visio) ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *RGPD : les changements à prévoir, comment se conformer sur la protection des données personnelles ?*

RGPD : Obligations des pharmacies



RGPD : Obligations des pharmacies

Tous les établissements de santé sont concernés par le RGPD en tant que responsables de traitement de données personnelles dans leur organisme, et parfois également comme sous-traitants (dans le cadre d'un groupement par exemple) ;

Pour rappel, l'article 35 du RGPD (Règlement Européen sur la Protection des Données personnelles) indique :

« Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro. »

Le RGPD porte sur toutes les données personnelles issues des activités de l'établissement de santé, et pas uniquement sur les données de santé générées par la prise en charge des personnes ;

De nombreuses actions sont à mener dès à présent, y compris pour les établissements qui disposent déjà d'un correspondant informatique et libertés (CIL). En effet, le règlement entre en application en mai 2018. Ces actions s'inscrivent dans la démarche globale de gestion des risques portée par l'établissement pour améliorer la qualité et la sécurité des soins, et s'intègrent notamment aux procédures de conformité de l'établissement, ainsi qu'à la gestion des risques de sécurité des systèmes d'information de l'établissement.

2 qualifications juridiques

D'une manière générale, l'établissement est responsable de multiples traitements de données personnelles, impliquant ou non des données de santé. Dans certains cas, l'établissement peut être considéré comme un sous-traitant, lorsqu'il agit pour le compte d'un tiers, notamment dans le cadre de certains groupements.

> L'établissement traite des données personnelles qui ne sont pas des données de santé (les données de ressources humaines par exemple) pour lesquelles le RGPD s'applique.

> L'établissement de santé collecte, gère et traite également des données de santé.

De façon identique au régime actuel, le RGPD fixe un principe d'interdiction de collecte de ces données en raison de leur sensibilité. Toutefois, ce principe est assorti de plusieurs exceptions, comme dans la loi Informatique et Libertés. A titre d'exemple, il est possible de créer un traitement de données de santé à caractère personnel lorsque la personne concernée donne son consentement exprès. Autre fondement possible utilisé dans le cadre de l'activité quotidienne des établissements de santé, les traitements créés pour une finalité relative :

- – aux diagnostics médicaux, à la prise en charge sanitaire ou sociale, ou à la gestion des systèmes et des services de soins de santé ;
- – à l'intérêt public dans le domaine de la santé publique, aux fins de recherche, de la médecine préventive ou de la médecine du travail.

Consultez la liste de nos formations et services sur le RGPD



RGPD - Règlement Général sur la Protection des Données

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 83041 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 ».

- Audit Sécurité (ISO 27001) ;
- Expertises techniques et judiciaires (avis techniques, technique de preuve numérique, disques durs, e-mails, contenus, détournements de données...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (investigation numérique et en cybersécurité)
- 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 : CNIL

La Cnil inflige une amende de 100 000 euros à Darty



La Cnil inflige une amende de 100 000 euros à Darty

Le groupe est sanctionné pour ne pas avoir suffisamment sécurisé les données des clients ayant eu recours au service après-vente en ligne.

En février 2017, la CNIL a été informée de l'existence d'un incident de sécurité concernant le traitement des demandes de service après-vente des clients de la société ETABLISSEMENTS DARTY ET FILS.

Lors d'un contrôle en ligne réalisé début mars 2017 les équipes de la CNIL ont pu constater qu'une défaillance de sécurité permettait d'accéder librement à l'ensemble des demandes et des données renseignées par les clients de la société, via un formulaire en ligne de demande de service après-vente. Plusieurs centaines de milliers de demandes ou réclamations contenant des données telles que les nom, prénom, adresse postale, adresse de messagerie électronique ou numéro de téléphone des clients étaient potentiellement accessibles.

Le contrôle sur place réalisé quinze jours plus tard a révélé que le formulaire de demande de service après-vente, à l'origine du défaut de sécurité, avait été développé par un prestataire commercialisant un logiciel de service après-vente « sur étagère ». Lors du contrôle, la société ETABLISSEMENTS DARTY ET FILS a indiqué avoir recours à un autre formulaire distinct et ne pas utiliser celui à l'origine de l'incident.

Les vérifications opérées par la CNIL ont pourtant permis de constater que les fonctionnalités du logiciel rendant accessible le formulaire développé par son prestataire n'avaient pas été désactivées. Elles ont également révélé que le prestataire n'avait pas mis en place de filtrage des adresses URLs, qui aurait permis d'empêcher à des tiers non autorisés d'accéder aux données des clients contenues dans l'outil de gestion des demandes de service après-vente via le formulaire défectueux.

Alors même qu'elle avait informé la société de cet incident de sécurité, la CNIL a constaté que les fiches des clients étaient toujours accessibles entre le premier et le second contrôle et que de nouvelles fiches avaient été créées dans ce laps de temps. Le soir même du second contrôle, la société l'informait des mesures prises pour remédier à cet incident.

La Présidente de la CNIL a désigné un rapporteur afin que soit engagée une procédure de sanction à l'encontre de la société ETABLISSEMENTS DARTY ET FILS.

La formation restreinte de la CNIL a prononcé une sanction d'un montant de 100.000 euros, estimant que la société avait manqué à son obligation de sécurité des données personnelles, en méconnaissance de l'article 34 de la loi Informatique et Libertés.

La formation restreinte a considéré que le simple fait que la société fasse appel à un prestataire sous-traitant ne la décharge pas de son obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement.

La société aurait dû s'assurer préalablement que les règles de paramétrage de l'outil mis en œuvre pour son compte ne permettaient pas à des tiers non autorisés d'accéder aux données des clients. Cette vérification préalable d'absence de vulnérabilité fait partie des tests élémentaires qui doivent être réalisés par une société en matière de sécurité des systèmes d'information.

Par ailleurs, en sa qualité de responsable de traitement, la société aurait dû procéder de façon régulière à la revue des formulaires permettant d'alimenter l'outil de gestion des demandes de service après-vente. A ce titre, la formation restreinte a considéré qu'une bonne pratique en matière de sécurité des systèmes informatiques consiste à désactiver les fonctionnalités ou modules d'un outil qui ne seraient pas utilisés ou pas nécessaires.

La formation restreinte a néanmoins tenu compte notamment de l'initiative du responsable de traitement de diligenter un audit de sécurité après cette atteinte à la sécurité des données ainsi que de sa bonne coopération avec les services de la CNIL.

Pour approfondir

> Délibération n°SAN-2018-001 du 8 janvier 2018 Délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire à l'encontre de la société ETABLISSEMENTS DARTY ET FILS Etat: VIGUEUR 

Faillle non réparée après un premier contrôle

La Commission révèle en avoir rapidement informé Darty. Pourtant « la Cnil a constaté que les fiches des clients étaient toujours accessibles entre le premier et le second contrôle et que de nouvelles fiches avaient été créées dans ce laps de temps ».

Cette faille provenait en fait d'un logiciel de service après-vente proposé par un sous-traitant. Mais la Cnil a considéré « que le simple fait que la société fasse appel à un prestataire sous-traitant ne la décharge pas de son l'obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement »...[lire la suite]

Consultez la liste de nos formations et services sur le RGPD



RGPD = RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

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 spécialisée 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, contenus, détournements de clientèle...);

• Expertises de systèmes de vote électronique ;

• Formations et conférences en cybercriminalité ; (Autorisation de la DITEF n°93 84 03041 84)

• Formation de C.I.L. (Correspondants Informatique et Libertés) ;

• Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous



Réagissez à cet article

Source : *DARTY : sanction pécuniaire pour une atteinte à la sécurité des données clients*

RGPD : Comment gagner la confiance des clients ?



L'entrée en vigueur imminente du Règlement Général sur la Protection des Données Personnelles (RGPD), en mai 2018, va considérablement modifier la façon dont les entreprises gèrent, stockent et sécurisent les données de leurs clients. Destiné à unifier les politiques de protection des données des différents pays européens, il prévoit en effet plusieurs points essentiels parmi lesquels le droit à l'oubli, un profilage client plus restreint, plus de transparence sur l'utilisation des données et l'obligation de faire part dans les 72 heures de toute violation constatée.

L'année écoulée a été marquée par plusieurs grosses affaires de violation de données, telle que la cyberattaque d'Uber, qui ont mis sur le devant de la scène les questions de confidentialité et de sécurité des données client. Sensibilisés par ces événements, les consommateurs souhaitent plus que jamais être rassurés au sujet de la protection de leurs informations personnelles. Ainsi, à en croire une récente étude réalisée par l'ICO*, 80 % des Britanniques ne font pas confiance aux organisations à cet égard. Si cette méfiance s'explique en partie par une mauvaise compréhension de l'utilisation qui est faite de leurs données, comme chez 92 % des sondés, le besoin de transparence est évident. La confidentialité des données, plus qu'un simple détail annexe, doit véritablement être intégrée à la structure même de l'entreprise.

En permettant aux organisations de prouver qu'elles ne prennent pas à la légère les données qui leur sont confiées et qu'elles n'utiliseront ces dernières que pour améliorer la relation qu'elles entretiennent avec leurs consommateurs, le RGPD va certainement favoriser la confiance et l'engagement client.

C'est en effet toute la relation client qui va changer et se renforcer : en ayant la possibilité de donner (ou non) son consentement quant à la possession et à l'utilisation de ses données par l'entreprise, la finalité de cette utilisation, la durée de stockage, le lieu de traitement et le recours dans la prise de décision automatisée, entre autres, le consommateur sera désormais beaucoup plus impliqué. Il sera aussi plus enclin à poursuivre sa relation avec les marques qui auront rapidement devancé l'appel du RGPD...[lire la suite]



LE NET EXPERT

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - 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 ;

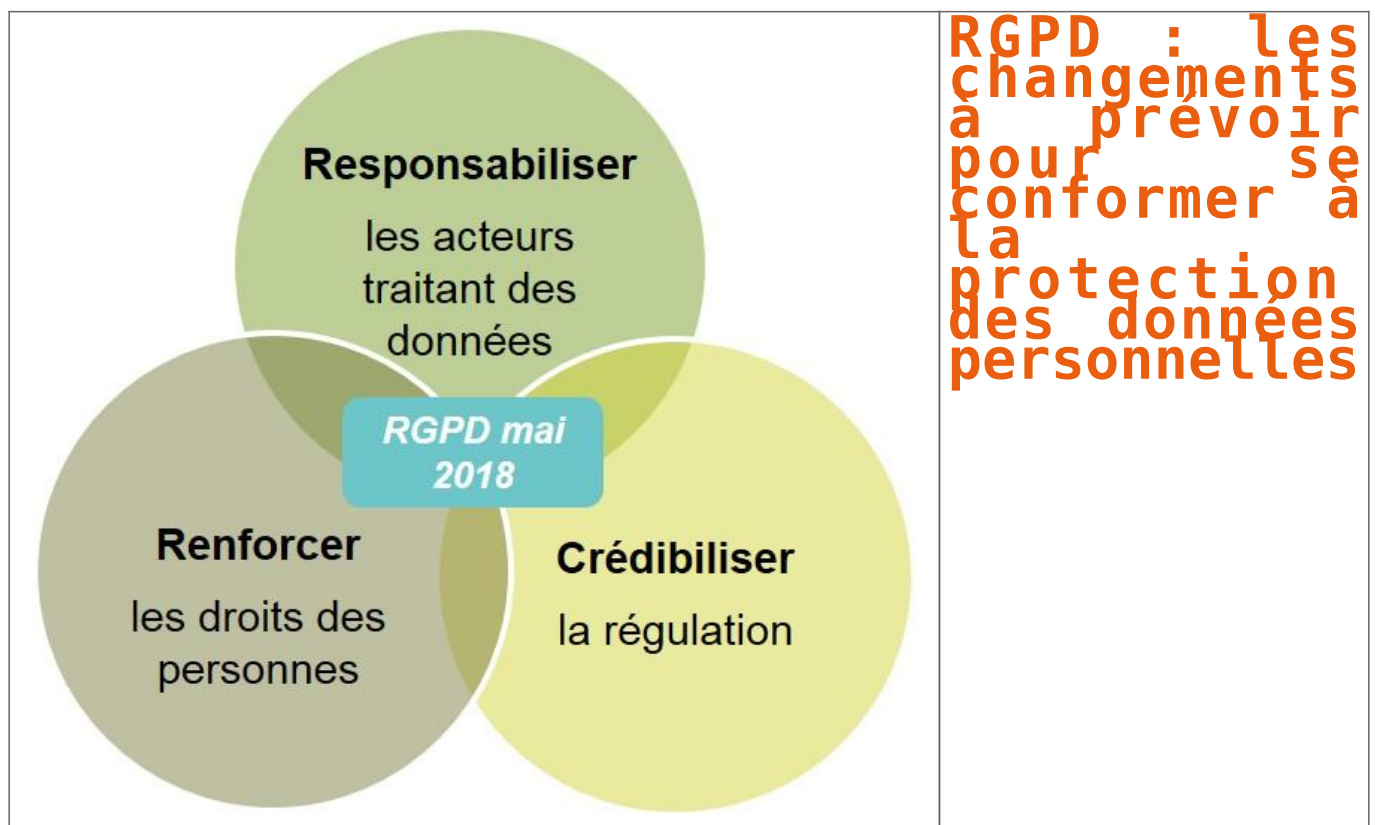


Contactez-nous



Réagissez à cet article

RGPD : les changements à prévoir pour se conformer à la protection des données personnelles



A partir du 25 mai 2018, toutes les entreprises gérant et collectant des données sur les personnes devront respecter chacune des obligations du Règlement européen pour la protection des données, le RGPD. Toutes les entreprises sont donc concernées par ce règlement que vous fassiez de l'outbound ou de l'inbound marketing. Le règlement prévoit également de lourdes sanctions en cas de violation de clauses : votre entreprise est-elle prête ?

1-QU'EST-CE QUE LE RGPD ?

Le Règlement général pour la protection des données – RGPD – a été adopté par le Parlement européen le 4 avril 2016. En anglais il est le GDPR pour « General Data Privacy Regulation ». Il vise à protéger toutes les données à caractère personnel des individus au sein de l'Union Européenne à travers **trois objectifs ambitieux** et précis :

- L'uniformisation européenne de la réglementation sur la protection des données
- La responsabilisation des entreprises
- Le renforcement du droit des personnes

Responsabiliser
les acteurs
traitant des
données

RGPD mai 2018

Renforcer
les droits des
personnes

Crédibiliser
la régulation

Le règlement n'a besoin d'aucune disposition légale en fonction du pays de l'entreprise : son application concerne directement tous les pays européens, à partir d'un même texte. L'intérêt majeur de cette uniformisation à échelle européenne est la simplification des mesures, centralisées vers un interlocuteur unique. Les entreprises pourront s'adresser directement à l'autorité de protection des données pour l'Etat membre dans lequel se situe l'établissement principal. La simplification des formalités pour les entreprises doit aussi permettre de les responsabiliser dans le traitement et la gestion des données. Les rôles, les responsabilités, les fonctions sont réparties et précisées, avec un ensemble de points à suivre : chaque entreprise doit mettre en place une politique de protection des données personnelles, et s'assurer qu'à chaque étape de la gestion des données, le RGPD est respecté. De nouveaux droits sont introduits, comme le droit à la portabilité, qui permet aux personnes de récupérer les données fournies, pour un contrôle total de ses propres données. On peut citer aussi le droit à réparation des dommages matériels et moraux, des droits spécifiques pour les enfants et le traitement de leurs données, des droits aux recours collectifs.

Consultez la liste de nos formations et services sur le RGPD



2 – LE RGPD, POUR QUI ?

Le RGPD est applicable sur toutes les données à caractère personnel de chacun des citoyens et résidents européens, soit « toute information se rapportant à une personne physique identifiée ou identifiable » selon la définition du RGPD. Il permet même de faire valoir ses droits face à une entreprise non européenne.

Dès lors qu'une entreprise européenne traite des données personnelles – noms, e-mails, numéro de téléphone... elle est concernée. Collecte, enregistrement, conservation, classement, utilisation, diffusion... le RGPD s'applique aux entreprises privées comme publiques des 28 Etats-membres de l'Union européenne, ou pour être plus précis :

- Aux entreprises proposant des biens et des services sur le marché européen
- Aux entreprises collectant des données à caractère personnel sur les résidents de l'UE
- Aux entreprises non implantées dans l'UE, dès qu'elles collectent et traitent de données personnelles appartenant à un résident de l'Union européenne.[lire la suite]

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 EUROPEEN 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 83841 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 spécialisée 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, conteneurs, détournements de clients...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Auteurs de livres et articles)
- Formation de C.I.L. (Correspondant 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 : *RGPD : les changements à prévoir, comment se conformer sur la protection des données personnelles ?*

La protection des données personnelles a 40 ans. Retour sur ses origines en vidéo



La protection des données personnelles a 40 ans. Retour sur ses origines en vidéo

A l'occasion de ses 40 ans, la CNIL vous propose une sélection d'archives vidéos concoctée par l'INA !
Ces temps-forts télévisuels retracent l'action de la CNIL et les grands sujets qui ont marqué son histoire.

Consultez la liste de
nos formations et
services sur le RGPD



RGPD = RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

LE NET EXPERT

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - 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](#)



Réagissez à cet article

RGPD : Faire face aux exigences

Denis JACOPINI  vous informe	RGPD : Faire face aux exigences
--	--

À compter du 25 mai 2018, le nouveau règlement européen relatif à la protection des données personnelles connu sous l'acronyme RGPD s'appliquera à toutes les entreprises publiques ou privées.

Ces dernières devront entrer dans une démarche proactive de mise en conformité du nouveau règlement. L'enjeu est de taille, car tout manquement à ces nouvelles obligations pourrait être lourdement sanctionné par l'autorité de contrôle, la CNPD, qui sera habilitée dès l'entrée en vigueur du règlement à infliger des amendes allant jusqu'à 20 millions d'euros et 4 % du chiffre d'affaires mondial.

Le champ d'application du RGPD est particulièrement large : toutes les entités, européennes ou non, sont concernées à partir du moment où elles collectent et effectuent des traitements de données à caractère personnel d'un citoyen européen. Le RGPD vient renforcer les droits de la personne, et par conséquent augmenter les devoirs et les responsabilités de toute la chaîne d'acteurs, du responsable de traitement aux partenaires commerciaux, y compris les sous-traitants fournisseurs de services.

Tous les flux de données sont concernés par cette nouvelle réglementation.

Ces nouvelles contraintes s'appuient notamment sur le principe d'accountability qui impose à chaque entreprise une obligation de rendre compte, notamment en se dotant d'une politique globale de protection des données conforme à la réglementation, et en étant à même de prouver à tout moment que des mesures concrètes et des procédures adéquates ont été mises en place. Dans ce nouveau contexte, il est préconisé que les responsables de traitement aient recours à des prestataires externes leur permettant d'assurer une mise en conformité effective...[lire la suite]

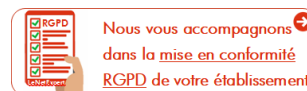
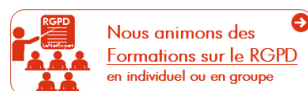
Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec 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, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.
« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

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

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

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)

Le RGPD (GDPR en anglais) : une réglementation que doivent aussi suivre vos sous-traitants



Le nouveau règlement européen sur la protection des données personnelles doit entrer en vigueur en mai 2018. Les donneurs d'ordre des métiers de service ont préparé leur mise en conformité et pressent leurs sous-traitants de faire de même. Cela représente pour eux de nouvelles charges à assumer.

Denis JACOPINI nous rappelle un extrait des termes de l'article 28 du RGPD (Règlement Européen sur la Protection des Données) :

Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Le traitement par un sous-traitant est régi par un contrat [...] prévoit, notamment, que le sous-traitant:

- a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;
- b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;
- c) prend toutes les mesures requises en vertu de l'article 32;
- d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant;
- e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;
- f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant;
- g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel; et
- h) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

Ainsi, même si vous êtes en règle vis à vis du RGPD mais si votre sous-traitant ne l'est pas, le résultat pourrait bien être équivalent comme si vous n'étiez pas en règle.

La mise en conformité du sous-traitant requiert d'abord une mise à niveau des mesures organisationnelles et techniques de cyber sécurité, avant de se concentrer sur la gestion des données personnelles. Les PME et ETI ont souvent fait l'impasse sur ce domaine générateur de coûts, pensant, grâce à leur petite taille, d'échapper aux attaques les plus graves. Aujourd'hui avec les puissants moyens d'information, ce n'est plus le cas, un pirate peut appréhender une filière et frapper le maillon le plus faible...[lire la suite]

LE NET EXPERT

• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)

- ANALYSE DE VOTRE ACTIVITÉ

- CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES

- IDENTIFICATION DES RISQUES

- ANALYSE DE RISQUE (PIA / DPIA)

- 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).



- **Mise 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 : *Le GDPR, un risque pour les PME en position de sous-traitance ?*