

**Editeurs de logiciels:
pourquoi vos clients vont
vous contraindre à justifier
de la conformité au RGPD de
vos outils ?**



Editeurs de
logiciels:
pourquoi
vos clients
vont vous
contraindre
à justifier
de la
conformité
au RGPD de
vos outils
?

Les éditeurs de logiciels devront dorénavant faire la démonstration de la conformité de leurs solutions au Règlement général de protection des données, lequel entrera en vigueur le 25 mai 2018.

La Cnil a eu l'occasion de l'affirmer à plusieurs reprises, et le règlement européen général en matière de protection des données (RGPD) ne change rien à la situation sur ce point: les éditeurs de logiciels ne sont pas considérés comme responsables de traitement. Seuls les clients utilisateurs le sont par principe. Mais alors, pourquoi les éditeurs font-ils face à des demandes urgentes de leurs clients, les pressant de fournir des preuves de la conformité de leurs produits au RGPD? Le règlement européen modifie le management de la conformité en imposant l'accountabilité. Les responsables de traitement doivent donc, dorénavant, démontrer leur conformité. L'accountabilité implique pour les responsables de traitement de déterminer des mesures techniques et organisationnelles permettant de démontrer que les traitements qu'ils mettent en oeuvre sont conformes au RGPD.

L'importance du programme de management de la conformité

L'accountabilité nécessite de déterminer un programme de management de la conformité en matière de protection des données. Ce programme doit contenir notamment une procédure de violation des données, des politiques de sécurité et de durée de conservation mais également des procédures permettant de s'assurer que les principes de protection par défaut et dès la conception sont appliqués. Si la protection dès la conception pour un responsable de traitement lui impose de déterminer les règles et fonctions nécessaires à la protection des données pour les outils qu'il crée ou développe en interne, il doit également vérifier, lorsqu'il acquiert des droits d'utilisation d'un outil édité par un tiers, que cet outil intègre l'ensemble des fonctions, paramètres et spécifications requis pour respecter les obligations du RGPD. Cela signifie, pour les outils qu'ils prennent sous licence, que les responsables de traitement doivent exiger de leurs éditeurs qu'ils attestent de la conformité de leurs produits. Ainsi, les responsables de traitements sont à même de démontrer qu'ils respectent leurs propres obligations...[lire la suite]

Commentaire de Denis JACOPINI

Depuis plusieurs années, les éditeurs de logiciels auraient dû assurer l'évolution de leurs logiciels par rapport à la réglementation en général et la protection des données personnelles en particulier.

En effet, depuis plus de 30 ans, les données inutilisées doivent faire l'objet d'une anonymisation ou d'une suppression. Quel éditeur de logiciel dispose de cette fonction de suppression ou d'anonymisation par rapport à une date de dernière utilisation? Non seulement quasiment aucun, mais ceux à qui leurs clients leur demandent de respecter la réglementation en général envoient en retour pour les plus audacieux un insolent devis, et une réponse négative pour les plus téméraires. Heureusement que l'évolution de la réglementation au travers du RGPD va faire évoluer les choses par la force, car ce n'est pas au client final ni de payer les évolutions réglementaires des logiciels ni la résolution des dysfonctionnements en cachant l'amélioration de leurs failles dans des mises à jour payantes.

Accepteriez-vous que votre garage vous fasse payer la réparation des défauts de fabrication de votre voiture ?

A Lire aussi :

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 : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Enseignements de la sécurité (en français et en anglais) ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : [Tribune] Editeurs de logiciels: pourquoi vos clients vont vous contraindre à justifier de la conformité au RGPD de vos outils?