URL :http://www.zdnet.fr/
PAYS :France
TYPE :Web Grand Public

► 4 décembre 2017 - 10:17

> Version en ligne

La formation des collaborateurs au RGPD, un enjeu-clé

La formation des collaborateurs au RGPD, un enjeu-clé : Technologie: La conformité au RGPD passe par une sensibilisation de tous les employés aux enjeux de la protection des données personnelles. L'accent doit être mis sur les populations les plus exposées aux risques. La culture de la data privacy peine à s'installer dans les entreprises. 64% des collaborateurs s'estiment insuffisamment sensibilisés aux enjeux du RGPD selon une récente enquête **d'Optimind** Winter – OpinionWay sur l'état d'avancement des chantiers de mise en conformité au futur règlement européen sur la protection des données personnelles. Un gros trou dans la raquette à moins de six mois de l'échéance. La contribution active des salariés en matière de confidentialité des données est, en effet, un prérequis essentiel de la bonne application du nouveau cadre réglementaire. Dans son article 39, le RGPD rappelle que l'une des missions du délégué à la protection des données (DPO) porte justement sur la sensibilisation et la formation du personnel participant aux opérations de traitement. Plusieurs autorités de contrôle ont, par ailleurs, souligné que l'adoption de la norme ISO 27001 démontre une intention manifeste de l'organisation certifiée à se conformer au RGPD. Dédiée au management de la sécurité de l'information, cette norme cite, parmi ses bonnes pratiques, la sensibilisation des utilisateurs. Effectivement, à quoi bon mettre en place les dispositifs techniques et les process organisationnels les plus robustes si les salariés ne les appliquent pas ? Comment pourraient-ils se conformer à des règles dont ils n'ont même pas eu connaissance ? Le RGPD peut être d'ailleurs l'occasion de lutter contre le shadow IT et de mieux encadrer l'usage du byod. Formation pour tous sur les grands enjeux de la privacy Pour sensibiliser les salariés aux enjeux de conformité, une entreprise peut utiliser toute la palette des outils de la communication interne (intranet, newsletter, affichage...) et de formation (sessions en présentiel, e-learning, tutoriels vidéos…). Conscio Technologies a lancé un cursus de sensibilisation sur le RGPD à base de vidéos, de saynètes et de quizz pour valider les acquis. Pour son PDG, Michel Gérard, il convient de mettre en place une offre à tiroirs afin de toucher les différents publics. En commençant par les basiques qui concernent potentiellement tout l'effectif. « Tout le monde peut, à un moment ou à un autre, être amené à manipuler des informations sensibles. Il convient de rappeler ce qu'est une donnée personnelle et les enjeux de protection derrière. » Un fichier Excel créé à titre individuel, hors du radar de la DSI, est un traitement en soi. Certains CIL, comme celui de la Cnaf, interviennent dans les parcours d'intégration des recrues pour évoquer la réglementation dans ses grandes lignes. Ces basiques de la conformité peuvent être complétés par une piqure de rappel sur les risques liés au piratage (phishing, fraude au président…) et les règles d'hygiène élémentaires à appliquer (gestion des mots de passe…). Selon Michel Gérard, l'accent doit être mis sur les actifs de la génération Y. Rôdés au numérique, ils en oublient parfois les contraintes en milieu professionnel adoptant des comportements à risques. Cette sensibilisation peut être couplé avec une réactualisation de la charte utilisateurs rappelant que la responsabilité du collaborateur peut être engagée en cas de non-respect, entraînant un avertissement voire un licenciement pour faute. « Les collaborateurs ne pourront pas dire qu'ils ne savaient pas. La formation a au moins ce mérite. » Formations spécifiques pour les populations à risques Un cran plus loin, on trouve les formations destinées aux populations les plus exposées. A savoir les RH, le marketing et les achats. Au sein de la DRH, les chargés de recrutement ne peuvent constituer une CVthèque à partir de LinkedIn et Viadeo même si les candidats ont rendu leurs profils sociaux publics. En ce qui concerne le marketing et les services support, l'attention sera portée sur les commerciaux et les opérateurs de la relation client qui renseignent les champs en texte libre dans les solutions de CRM afin d'éviter toute observation illicite sur la religion ou l'orientation sexuelle d'un individu. Enfin, les acheteurs doivent passer en revue les contrats des sous-traitants et les appels d'offre afin de s'assurer de leur conformité. Changer la façon de conduire les projets IT Une autre population doit particulièrement concentrer l'attention : les équipes de la DSI. Là, il s'agit de changer ni plus ni moins la façon de conduire les projets en intégrant le respect de la vie privée dès la conception d'une base de données, d'une application ou d'un service puis de fixer le niveau de sécurisation le plus élevé selon les principes

URL :http://www.zdnet.fr/
PAYS :France
TYPE :Web Grand Public

► 4 décembre 2017 - 10:17

> Version en ligne

de « privacy by design » et de « privacy by default ». Du développeur à l'administrateur en passant par le chef de projet, tout le monde est concerné. A un autre niveau, on trouve les formations dédiées aux responsables de traitement. Ils doivent intégrer les nouvelles obligations qui leur incombent comme la tenue du registre des traitements ou le mise en œuvre d'études d'impacts. Sont concernés le gérant de la société qui a une responsabilité juridique mais aussi ses adjoints qui ont, eux, une responsabilité opérationnelle dans la mise en place de traitements. Enfin, il y a les cursus dédiés au DPO. La Cnil propose des ateliers pour aider les Correspondants informatique & libertés à se mettre à niveau afin d'occuper le poste. Le cabinet Anaxil-DPMS dispense des formations certifiantes. L'école d'ingénieurs Isep propose, de son côté, un mastère spécialisé management et protection des données à caractère personnel particulièrement prisé.
Pour aller plus loin sur ce sujet Comment les entreprises françaises perçoivent le RGPD ? RGPD : le retour d'expérience très instructif de la Cnaf Jean Lessi (Cnil) : « Le 25 mai 2018 n'est pas une date couperet » RGPD : l'opportunité de lutter contre le shadow IT Avec le RGPD, comment mieux encadrer le Byod RGPD : comment tenir un registre des traitements Périmètre, missions : le portrait-robot du DPO Le CIL est légitime à devenir DPO… sous conditions Etes-vous prêts pour le RGPD ? Voici la check-list ! Les 3 grands principes du RGPD