10 conseils pour préparer votre organisation au RGPD

Le 18 avril 2017 - Le RGPD (Règlement Général sur la Protection des Données), qui entrera en vigueur le 25 mai 2018, aura non seulement un impact sur tous les pays membres de l'Union Européenne mais aussi sur les pays qui traitent des données concernant les citoyens de l'UE.

Bien que la mise en vigueur effective de cette réglementation ne se produise que dans un peu plus d'un an, DMA a mené une enquête démontrant que plus d'un quart (26%) des dirigeants pensent que leur entreprise n'est pas préparée au RGPD. Dès lors, que peuvent faire les entreprises pour s'assurer qu'elles sont en conformité ? Voici 10 conseils très simples que les entreprises peuvent suivre.

1. 1. Organiser la mise en conformité

L'an dernier, dans un blog, Steve Wood, chef de la stratégie et de l'information internationale au Bureau du Commissaire à l'Information (ICO), a modéré les préoccupations au sujet du Brexit en affirmant « qu'une fois implémentée dans l'UE, le RGPD sera d'application pour de nombreuses organisations au Royaume-Uni ».

Bien que le Royaume-Uni se prépare à quitter l'UE, un grand nombre de ses entreprises et organisations devront pourtant se conformer au RGPD car elles travailleront encore avec des données de citoyens de l'UE.

Concernant les autres pays de l'UE, il sera bien entendu important pour toutes les organisations qui traitent des données concernant les citoyens de l'UE de planifier en amont l'intégration de ce nouveau règlement. Il convient dès lors de mettre en place un plan d'action pour la mise en conformité avec la loi, et ce, en commençant par cartographier les données et les risques qu'elles encourent.

2. 2. Sensibiliser les collaborateurs

Il est important que tous les décisionnaires d'une organisation soient informés des implications du RGPD et de ce que cela représente pour leurs activités quotidiennes.

Selon l'enquête Gigamon 2017, seulement 41% des professionnels de l'IT ont déclaré être « complètement informés » des implications du RGPD alors que 9% a indiqué n'en avoir aucune idée.

Ces chiffres démontrent clairement qu'il y a encore beaucoup de travail et d'efforts à faire pour que toutes les organisations soient réellement bien informées.

De plus, informer et éduquer l'ensemble des salariés de son organisation sur la modification des usages, va devenir essentiel afin d'éviter les mauvaises pratiques.

3. 3. Déterminer la façon dont une organisation traite les données

Sous la Directive de Protection des données de l'UE actuelle, ce ne sont que les contrôleurs de données qui sont responsables de la conformité en matière de protection des données.

Cependant, comme l'explique ICO, le RGPD place également des obligations statutaires directes sur ceux qui traitent les données. Il est donc important d'établir si une organisation n'effectue que du traitement de données ou que du contrôle tout en gardant à l'esprit qu'elle pourrait faire les deux.

Effectuer un audit des méthodes utilisées actuellement est une des meilleures façons de se préparer au RGPD. Cela signifie qu'une compréhension approfondie de la manière dont une organisation traite les données est primordiale.

4. 4. Examiner toutes les facettes du traitement des données dans une organisation

Il est important de savoir où les données personnelles sont stockées avant d'évaluer la sécurité de cet endroit, ainsi que d'être informé sur la ou les personnes en charge du contrôle de ces données. Il est d'une crucial d'impliquer le département IT dans ce processus afin d'avoir des précisions supplémentaires et d'avoir une meilleure évaluation des ressources réelles de son organisations.

5. 5. Examiner les violations de données antérieures

Examiner toutes les violations et/ou fuites de données antérieures fournira une image précise des capacités d'une organisation à réagir à des attaques futures et donnera une meilleure idée des possibilités qu'offrent les procédures existantes pour répondre à des exigences futures.

Une des mesures exceptionnelles qui sera introduite par le RGPD est la notification suite à une fuite de données. Les organisations devront signaler ces violations/fuites dans un délai maximum de 72 heures après leur découverte. Elles devront être accompagnées d'informations sur la nature et le degré de sévérité de l'attaque.

Les amendes et sanctions en cas de non-conformité seront importantes (2 à 4% du chiffre d'affaires annuel ou 20 à 40 millions d'€) et visent à motiver les organisations à s'impliquer dans leur mise en conformité.

6. 6. Nommer un Data Protection Officer (DPO)

Selon l'IAPP, les Data Protection Officers seront indispensables pour le secteur public ou les organisations qui traitent régulièrement et à grande échelle des données personnelles. Le DPO travaille de manière indépendante et rapportera au plus haut niveau de direction dans l'organisation. Sa principale responsabilité est d'avoir une compréhension parfaite du RGPD et d'implémenter les exigences requises afin d'obtenir l'accord de toutes les parties impliquées.

7. 7. Etre informé en matière de règles concernant le droit des personnes

Un des éléments clefs de la GDPR est le renforcement du droit des personnes concernées, y compris le droit à l'oubli et la portabilité des données. Ceci signifie qu'une organisation peut être amenée à fournir des données qui iront à la concurrence.

Les entreprises étant obligées de promouvoir ces droits, il est important que des procédures permettant cette portabilité soient mises en place.

8. 8. Etre informé en matière de consentement

Le RGPD vise à fournir plus de clarté en ce qui concerne la question du consentement. De nouvelles mesures rendent obligatoires l'obtention d'une déclaration explicite et claire de la part des personnes concernées qui fait preuve d'accord pour traiter des données personnelles.

Les entreprises seront soumises à de nouvelles mesures limitant le consentement donné par des enfants en matière de traitement de données sans accord parental. Il est donc important d'examiner les pratiques existantes et mettre en place des procédures d'informations sur la manière dont les données personnelles des individus seront utilisées et traitées.

9. 9. Identifier l'autorité de contrôle principale – le principe de « guichet unique »

De nombreuses organisations affectées par le RGPD ont des activités internationales et peuvent donc être soumises à des directives autres que le RGPD.

Il peut être difficile de déterminer quelle est l'autorité qui joue le rôle d'interlocuteur principal en matière de protection des données lorsqu'une plainte est soumise. Selon l'article 56 du RGPD, ceci est déterminé par le pays dans lequel siège l'organisation. Cela peut poser problème pour les entreprises qui disposent de plusieurs sites. S'il y a une incertitude, il est important d'établir le lieu où sont prises les décisions importantes en matière de traitement des données. Ce lieu fera office de siège décisionnel pour les affaires liées au RGPD et l'autorité de contrôle du pays en question sera désignée comme autorité principale.

10. Affecter plus de ressources

Toutes ces considérations peuvent peser lourdement sur l'infrastructure d'une organisation. Il est donc indispensable que les entreprises affectent des ressources supplémentaires afin de répondre à ces demandes.

Le livre blanc de WLS explique que sans planification préalable, « les entreprises pourraient être forcées de répondre aux nouvelles exigences sans avoir prévu les ressources nécessaires pour être en conformité » .

Affecter des ressources financières et humaines dès le début du processus est une excellente manière d'alléger toute pression potentielle ultérieure.

Pour plus d'information sur le RGPD et apprendre comment ESET peut aider les entreprises à se conformer à la nouvelle loi, visitez le site spécialement conçu pour le RGPD.

En savoir plus à propos d'ESET ?

Depuis 30 ans, ESET® développe des solutions de sécurité et des services d'avant-garde pour les entreprises et les consommateurs du monde entier. Avec des solutions qui vont de la sécurité endpoint et mobile jusqu'au chiffrement et à l'authentification à deux facteurs, les produits d'ESET, très performants et faciles à utiliser, offrent la tranquillité d'esprit aux consommateurs et aux entreprises en leur permettant de bénéficier de tout le potentiel de leur technologie. ESET protège et contrôle discrètement 24/7, met à jour - en temps réel - la protection afin que les utilisateurs soient en sécurité et que les entreprises puissent travailler sans interruption. Les menaces qui évoluent exigent un fournisseur de sécurité IT qui évolue, lui aussi. Supportée au niveau global par des centres de R & D, ESET est le premier fournisseur à obtenir plus de distinctions (100 Virus Bulletin VB100) en identifiant chaque malware "in-the-wild" sans interruption depuis 2003. Visitez www.eset.com pour plus d'information ou suivez-nous sur LinkedIn, Facebook et Twitter.

INFORMATION PRESSE

Vous désirez plus d'informations sur ESET ou tester un produit ? Contactez :

Catherine d'Adesky/Louise Biron — Maxime Mutelet

Key Communications — **MGK Technologies**

+32 2 230 40 72 — +352 26 18 51

catherine@keycommunications.be

louise@keycommunications.be

www.keycommunications.be — www.eset.lu