IDC et l'évaluation de la préparation au GDPR de Symantec

Ensemble des résultats de l'évaluation de la préparation au GDPR

IDC conçoit cinq étapes de préparation, avec des entreprises qui commencent au stade 1, et des entreprises qui en sont à la réalisation de la conformité au stade 5. Selon vos réponses à cette évaluation, votre entreprise est à **Étape 4 - Il faut optimiser**.

Par ailleurs, nous vous avons classé selon cinq stades dans chacun des trois domaines GDPR suivants pour que vous ayez une idée claire d'où vos efforts doivent être concentrés. Ces domaines sont les suivants :

- Approche globale du GDPR, objectif et leadership
- Objectif & connaissance des données
- Connaissance, évaluation et réduction des risques

Approche globale du GDPR, objectif et leadership

Le GDPR ne se limite pas à la sécurité informatique : il implique la manière dont l'entreprise aborde le concept et la culture de la confidentialité des données. Pour réussir, vous aurez besoin de l'engagement et du support de toute l'entreprise, de la direction générale aux unités commerciales individuelles. Favoriser une culture de responsabilité commune est essentielle pour atteindre une conformité durable sur le long terme.

Étape 2 - Il faut accélérer

Vous avez commencé le processus, mais il reste beaucoup à faire. Les entreprises qui sont dans cette phase de préparation se sont engagées à se conformer au GDPR mais sont encore dans la première moitié de leur parcours. Elles sont conscientes de l'ampleur des pénalités et sanctions proposées, mais sont souvent peu disposées à croire qu'elles seront appliquées.

Vous indiquez que vous vous êtes suffisamment engagé dans la mise en conformité au GDPR pour ne pas attirer l'attention du régulateur (probablement), mais vous limitez vos efforts à un programme pragmatique d'une activité précise. Cette stratégie est tout à fait raisonnable, au moins à court terme, tant qu'elle se fonde sur une analyse approfondie des activités. Votre objectif est d'être en conformité de manière pragmatique, vous devez donc être prêt à vous justifier face au régulateur en cas de problème.

En cas de doute, référez-vous toujours aux principes énoncés dans l'article 5 du GDPR. Soyez prêt à défendre votre position par rapport à ces principes : si vous êtes en mesure de le faire, vous éviterez les foudres du régulateur.

L'absence d'une équipe polyvalente de conformité ou d'un conseil de gouvernance avec de nombreux acteurs dans votre entreprise a diminué considérablement votre score de préparation. L'engagement de tous les acteurs concernés est essentiel pour réussir tout programme GDPR, et l'absence d'une telle approche concertée limite considérablement le succès final de toute activité de conformité. Envisagez de réexaminer cette situation dès que possible. Il est peu probable qu'une approche en silo du GDPR réponde aux principes fondamentaux requis par la nouvelle législation.

Connaissance des données

La gouvernance de l'information est la discipline sous-jacente qui permet la conformité au GDPR. La soumission de toutes les données personnelles à la gouvernance de l'information est obligatoire. Vous devez savoir quelles données personnelles vous possédez (selon la définition très large utilisée par le GDPR), ainsi que leur emplacement, consentement, durée de vie, et ainsi de suite. Démontrer au régulateur que vous avez une bonne maîtrise des données à caractère personnel est la première étape vers la conformité.

Étape 4 - Il faut optimiser

Vous êtes au stade avancé de la gouvernance et vous avez une confiance élevée en votre capacité à localiser toutes les instances de données à caractère personnel au sein de votre entreprise. Vous avez également une bonne compréhension des données à la fois structurées et non structurées, et êtes susceptible de vous conformer aux nouveaux droits d'accès, rectification, effacement et portabilité.

Vous faites partie de l'infime minorité d'entreprises qui ont entièrement confiance en leur capacité à identifier et localiser toutes les instances de données à caractère personnel au sein de leur entreprise. Bravo. Assurez-vous cependant que votre personnel ne crée pas de copies des données (probablement pour de bonnes raisons) qui ne sont pas conformes. Des copies de données sont effectuées fréquemment, pour des rapports, analyses, sauvegardes et autres. Assurez-vous que des processus sont installés pour éviter que cela se produise à l'avenir.

Vous connaissez très bien vos données. C'est bien : une condition préalable à la conformité au GDPR est de connaître les données que vous possédez et leur emplacement, ainsi que de savoir pourquoi vous les possédez. Cela est nécessaire pour compiler un dossier de traitement des données, en vertu de l'article 30. Vous devrez également éviter toute violation des principes de limitation de la finalité, limitation des données et limitation de conservation.

Que faire maintenant ? Concentrez-vous sur les lacunes concernant vos connaissances des données et leur emplacement. Comprendre les raisons pour lesquelles vous détenez ces données (limitation de la finalité) est également important, tout comme comprendre que des réglementations différentes s'appliquent à différentes catégories de données (telles que les catégories spéciales et les données relatives aux enfants).

Par-dessus tout, rappelez-vous que les régulateurs tolèreront les infractions et non-conformités mineures. En revanche, ils ne tolèreront pas une absence évidente d'efforts. Il ne suffit pas de connaître vos données : vous devez être en mesure de démontrer cette connaissance.

Connaissance, évaluation et réduction des risques

Tout est une question de risques avec le GDPR. La plupart de ses exigences ne sont pas normatives, ce qui signifie que les entreprises doivent décider des approches à adopter. Comment trouver le juste équilibre entre la collecte de données pour analyse et un risque accru dû à la minimisation des données et la limitation de la finalité ? Qu'est-ce qu'être « à la pointe de la technologie » et comment savoir si j'en ai besoin ?

La connaissance des risques commence par une introspection : quelles données ai-je en ma possession et comment les nouvelles réglementations changent-elles la manière dont je dois traiter ces données ?

Étape 2 - Il faut accélérer

Vous semblez être au stade de développement de la connaissance des risques, et êtes prêt à accélérer. Vous semblez vous impliquer en posant les bonnes questions, et ces dernières sont de plus en plus poussées. Vous rencontrez des difficultés avec certaines exigences plus avancées, et semblez justement préoccupé par l'augmentation des niveaux de risques associés au GDPR. Cependant, vos difficultés à donner la priorité à l'allocation de ressources doivent vous alerter sur l'importance des connaissances, notamment au niveau du conseil d'administration.

Votre réponse indique une approche avancée en matière de Cloud et de protection des données. Il faudra peut-être adapter les services Cloud existants pour s'assurer qu'ils respectent les nouvelles réglementations. À moins que vous vous êtes déjà assuré que votre utilisation du Cloud est conforme et ne nécessite pas d'autres modifications. Si cela est le cas, bravo : vous avez une longueur d'avance. Attention cependant : les conséquences d'une mauvaise utilisation du Cloud, par exemple supposer que les fournisseurs de Cloud peuvent endosser votre responsabilité (ils ne le peuvent pas), pourraient être graves. Assurez-vous que vous avez vérifié vos contrats de Cloud et qu'ils sont conformes au GDPR.

Vous semblez avoir une bonne perspective du risque lié au GDPR. Cela signifie que vous avez entièrement compris les conséquences éventuelles de la non-conformité, non seulement en termes d'amendes possibles mais aussi en termes de réputation, recours collectifs et suspension de traitement des données. Mais vous contrôlez également la situation et votre état d'esprit montre que votre préparation est bientôt terminée : vous avez avancé comme prévu dans votre processus de mise en conformité au GDPR.