Cybersécurité : comment se préparer à la nouvelle législation de L'Union Européenne ?

Deux nouvelles lois de l'Union Européenne régissant la sécurité de l'information et la protection des données devraient être mises en application d'ici fin 2017. Elles auront un impact majeur sur la manière dont les entreprises des États membres de l'UE implémenteront des solutions et des politiques de sécurité, et signaleront des fuites de données.

La directive de « cyber-sécurité » SRI (Sécurité des Réseaux et de l'Information) et le RGPD (Règlement Général sur la Protection des Données) auront un certain impact sur les entreprises de toute taille au sein de l'UE. Ces législations s'attacheront à normaliser les règles de sécurité de l'information et de protection des données entre les États membres, dans le but d'accroître la protection et réduire le nombre de fuites de données dont elles sont victimes.

Présentation de la réglementation

La directive de « cyber-sécurité » NIS (Sécurité des Réseaux et de l'Information) oblige un large éventail d'entreprises du secteur privé à se conformer à de nouvelles exigences de sécurité et de signalement d'incidents. Elle stipule également que les « opérateurs d'infrastructures critiques, » c'est-à-dire les entreprises de services publics, les transports et les entreprises de services financiers, doivent déployer des mesures appropriées pour gérer les risques de sécurité et signaler les incidents graves à une autorité nationale ou à l'équipe d'intervention informatique d'urgence.

Le RGPD (Règlement Général sur la Protection des Données), unifie les règlementations de protection des données existantes dans les pays de l'Union Européenne sous une législation unique, en introduisant des directives sur la manière dont les entreprises devront gérer des informations personnellement identifiables. Il sera applicable à toutes les entreprises ayant des activités en Europe, que les données personnellement identifiables qu'elles gèrent soient stockées dans le périmètre de l'Union Européenne, ou non. Il élargit également la définition des « données personnelles » pour inclure les adresses de courrier électronique, les adresses IP et les contenus postés sur des sites de réseaux sociaux.

Signification pour les entreprises

L'élément clé ici est que ces directives et réglementations deviendront exécutoires. Les entreprises qui ne respecteront pas la directive NIS ou le RGPD risqueront d'être lourdement sanctionnées pour toute infraction. Les amendes proposées sont de 2% du chiffre d'affaires annuel mondial, jusqu'à 100 millions d'euros.

Tandis que la nouvelle législation permettra de renforcer la responsabilité des entreprises, elle leur donnera également la possibilité d'examiner leurs pratiques actuelles en matière de données et de cyber-sécurité. Elle permettra également aux DSI et aux DSSI de préparer des analyses de rentabilisation pour investissement dans les technologies de sécurité et de protection des données et

la formation, et dégager un avantage concurrentiel en renforçant leur posture de sécurité.

Certaines des propositions du RGPD reflètent la directive NIS en termes de systèmes et de données, et de pénalités pour les non-conformités. Mais le RGPD comporte beaucoup plus de détails en termes de réglementation du traitement des informations personnellement identifiables des citoyens européens. Les articles du RGPD qui auront le plus d'impact sur les entreprises se répartissent en sept catégories clés. Regardons chaque catégorie tour à tour, leurs principales implications, et les mesures requises pour les entreprises.

Application du RGPD

Toute entreprise proposant des biens ou des services dans un État membre de l'UE sera soumise à la législation, retirant toute ambiguïté quant à savoir si la législation de protection des données s'applique à un pays ou une région donnée. Toute entreprise exerçant une activité au sein de l'UE, et traitant des données personnelles des sujets de l'UE, devrait prendre des mesures pour faire en sorte qu'elle respecte les réglementations, au risque de subir des pénalités importantes.

Qu'est-ce que les données personnellement identifiables ?

La définition des données personnelles sera élargie en vertu du RGPD, comme suit : « toute donnée concernant une personne physique identifiée ou identifiable (personne concernée) ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à une ou plusieurs caractéristiques spécifiques d'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne. »

Pour minimiser les risques d'exposition, les entreprises doivent veiller à ce que soient collectées et traitées les seules données nécessaires à des fins légitimes. Il est également sage de traiter toutes les données sur les individus comme étant personnelles, et les protéger de manière appropriée. Elles doivent être stockées uniquement pour la durée nécessaire, et détruites ou supprimées de manière définitive lorsqu'elles ne sont plus nécessaires, conformément à une politique de rétention de données appropriée.

Sécurité et signalement d'incidents

En termes de sécurité, les réglementations actuelles suggèrent que les entreprises implémentent des mesures techniques de protection et des procédures administratives « appropriées », mais sans préciser ce qu'elles devraient être. Cependant, il est probable qu'elles devraient inclure des mesures reconnues telles que le chiffrement des données et les pare-feux, tandis qu'en matière de procédure, les entreprises devraient informer les régulateurs de données et les individus touchés dans les 72 heures, si les fuites font courir un risque aux données identifiables. Avec l'augmentation des risques de cyber-attaques et de fuites de données ciblant les entreprises, il est probable que les amendes initiales au titre de la nouvelle règlementation seront élevées. Cela signifie que les entreprises traitant de grandes quantités de données personnellement identifiables devraient développer des processus de protection des données, d'enquête et de remédiation.

Amendes et mise en application

Les régimes de protection des données actuels à travers l'UE comportent des différences notables quant aux sanctions et la mise en application entre les différents États membres. Le RGPD permettra d'éliminer les différences et d'introduire de lourdes sanctions à grande portée. Les amendes maximales proposées sont punitives : jusqu'à 100 millions d'euros ou 5% du chiffre d'affaires annuel mondial de l'entreprise. Des sanctions de cette ampleur signifient que la protection des données et l'atténuation des risques de fuites ne peuvent être laissées au hasard : les entreprises doivent assurer qu'elles possèdent des solutions, des procédures et des politiques de sécurité appropriées, au risque d'encourir de graves sanctions pour non-conformité.

Confidentialité dès la conception

La confidentialité dès la conception signifie que les entreprises doivent implémenter et appliquer des processus techniques et organisationnels pour assurer que seule la quantité minimale nécessaire de données personnelles soit traitée pour chaque activité spécifique, et que les données personnelles ne soient pas divulguées plus que nécessaire. Les entreprises doivent anticiper cela en intégrant la confidentialité et la protection des données dans leurs systèmes et leurs processus dès le départ, en chiffrant les données personnelles pour les protéger lorsqu'elles sont stockées, et en minimisant leur communication lors de leur utilisation.

Traitement et chaîne d'approvisionnement

La nouvelle législation signifie que la chaîne d'approvisionnement, des fournisseurs aux clients, peut être tenue conjointement responsable de la protection des données. Les entreprises ne seront pas en mesure de reporter ou d'éluder leurs responsabilités légales en matière de protection des données. Cela signifie que les entreprises traitant de grandes quantités de données personnellement identifiables doivent appliquer des mesures de protection des données, et auditer leurs partenaires afin d'assurer qu'ils traitent également les données personnelles en toute sécurité.

Gouvernance et directeurs de la protection des données

Le RGPD doit encore clarifier si les entreprises doivent nommer un directeur de la protection des données (DPD) pour gérer la conformité et les processus internes de protection des données. Dans tous les cas, les entreprises doivent se préparer à devoir gérer des tâches supplémentaires de protection des données, de gestion et de rapports, qui devront être effectuées en interne. Compte tenu de l'importance de ces tâches pour minimiser la responsabilité des entreprises, la personne qui les aura en charge devra occuper un poste de direction et devrait être prête à y consacrer beaucoup de temps.

Les nouvelles lois de l'Union Européenne régissant la sécurité de l'information et la protection des données auront un impact majeur sur la manière dont de nombreuses entreprises dans les États membres de l'UE implémenteront des politiques et des solutions de sécurité, et signaleront des incidents de fuites de données. Cependant, les entreprises devraient voir la nouvelle législation comme une occasion de revoir leurs pratiques actuelles en matière de cyber-sécurité. Pas seulement pour se conformer à la réglementation, mais également pour dégager un avantage

concurrentiel en renforçant leur niveau de sécurité.