Préparez-vous pour le RGPD

Cybersecurité pour la protection des données

PRÉPAREZ-VOUS POUR LE RGPD
Règlement Général sur la Protection des Données

Qu'est-ce que le RGPD ?

Le **Règlement Général sur la Protection des Données (RGPD)** ou GDPR en anglais est la réponse de l'Union Européenne aux exigences croissantes en matière de protection de la vie privée de la société européenne. L'objectif principal du RGPD est d'établir les données personnelles en tant que propriété et de transférer le contrôle de ladite propriété à l'individu ou à l'utilisateur, plutôt qu'à l'entreprise ou au fournisseur. En outre, le RGPD entrera en vigueur sous peu et de nombreuses entreprises ne sont tout simplement pas prêtes à respecter les normes d'utilisation plus strictes, de déplacement et de stockage des données clients. Analysons la portée complète du RGPD et ce que cela signifie pour votre stratégie Cloud.

Aperçu

Depuis plus de 20 ans, la protection des données personnelles a été une question importante dans l'Union Européenne (UE) et le RGPD récemment ratifié amène la protection des données à un plus haut niveau. En plus d'un nouvel ensemble d'exigences légales qui nécessitent des réponses organisationnelles et technologiques, le RGPD s'applique également aux organisations du monde entier qui collectent ou traitent des données sur les résidents de l'UE, y compris les résidents permanents, les visiteurs et les expatriés. Conformément aux normes énoncées dans le RGPD, la conformité réglementaire dépendra désormais de la localisation géographique des personnes dont les données personnelles ont été collectées - et non le lieu d'enregistrement de l'organisation qui a recueilli les données. Par conséquent, répondre à l'exigence du RGPD nécessitera une attention et une action sérieuses de toutes les organisations qui font des affaires en Europe (y compris le Royaume-Uni après le Brexit), tant dans l'UE que dans l'Espace Économique Européen (EEE).

Le RGPD donne également aux résidents de l'UE le droit de demander leurs données personnelles auprès d'organisations qui collectent et hébergent de telles données et de retirer leur consentement de leur utilisation, ordonnant ainsi la destruction des données personnelles. L'article 12 du RGPD, qui couvre les droits des personnes concernées et la transparence associée à la gestion de ces données, précise que toute demande d'accès ou de destruction de données personnelles doit être gratuite, facile à réaliser et doit être exécutée "sans délai injustifié et au plus tard dans un mois." Cependant, comme la plupart des organisations auront besoin de temps et d'un investissement important pour se conformer aux processus et aux capicités du RGPD, l'UE a prolongé la date de mise en œuvre jusqu'en mai 2018. Mais étant donné la portée et l'impact transformateur du RGPD, il est impératif que les organisations révisent - et très probablement refontent - la manière dont elles traitent aujourd'hui les données personnelles.

Points clés du RGPD

Un aperçu des principaux changements du

RGPD et de la façon dont ils diffèrent de la directive précédente.
L'objectif du RGPD est de protéger tous les citoyens de l'UE des violations de leur vie privée dans un monde de plus en plus axé sur les données et de ce fait très différent de celui de la directive antérieure en 1995. Bien que les principes clés de la confidentialité des données soient toujours conformes à la précédente directive, de nombreux changements ont été proposés aux politiques réglementaires; les points clés du RGPD, ainsi que les informations sur les impacts qu'il aura sur les entreprises sont présentés ci-dessous :

Portée territoriale accrue (Applicabilité géographique élargie)
Sans doute le plus grand changement dans le contexte réglementaire de la confidentialité des données est fourni avec la juridiction élargie du RGPD, car elle s'applique à toutes les entreprises qui traitent les données personnelles des personnes concernées résidant dans la zone géographique connue sous le nom de l'UE, quel que soit l'emplacement de l'entreprise. Auparavant, l'applicabilité territoriale de la directive était ambiguë et se référait au processus de données «dans le contexte d'un établissement». Ce sujet est apparu dans plusieurs cas de tribunaux de grandes instances. Le RGPD rend son applicabilité très claire : elle s'appliquera au traitement des données personnelles par les contrôleurs et les processeurs des données dans l'UE, que le traitement ait lieu ou non dans l'UE. Le RGPD s'appliquera également au traitement des données personnelles des personnes concernées par l'UE par un contrôleur ou un processeur non établi dans l'UE, où les activités concernent : l'offre de biens ou de services aux citoyens de l'UE (quel que soit le paiement requis) et le suivi des comportements qui se déroulent au sein de l'UE. Les entreprises non européennes traitant les données des citoyens de l'UE devront également avoir un représentant dans l'UE.

Penalités

Dans le cadre du RGPD, les organisations en infraction peuvent être condamnées à une amende jusqu'à **4% du chiffre d'affaires global annuel ou 20 millions d'euros** (la plus élevée des deux), qui est actuellement l'amende maximale pouvant être imposée pour les infractions les plus graves (par exemple, ne pas avoir suffisamment de consentement clients pour traiter leurs données ou violer les principes de la "Privacy by design"). Toutefois, des amendes seront prélevées en utilisant une approche à plusieurs niveaux, en fonction de la portée de la violation (par exemple, une entreprise peut être condamnée à une amende de 2% pour ne pas avoir les dossiers requis (article 28), ne pas avoir informé l'autorité de supervision et la personne concernée d'une violation de données ou ne pas avoir effectué d'évaluation d'impact). Il est important de noter que ces règles s'appliquent à la fois aux contrôleurs et aux processeurs - ce qui signifie que les fournisseurs de services Cloud ne seront pas exemptés de l'exécution du RGPD.

PRÉPAREZ-VOUS POUR LE RGPD
Règlement Général sur la Protection des Données

Consentement

Le RGPD a également l'intention d'exiger la simplification des termes et conditions, puisque les récents termes et conditions sont devenus des sites remplis de notions légales illisibles visant à protéger l'initiateur plutôt que d'informer réellement le client. Le nouveau règlement exigera que les termes et conditions, ainsi que les demandes de consentement pour le traitement des données soient intelligibles et sous une forme facilement accessible, en utilisant un langage clair et simple. En outre, la capacité de retirer son consentement doit également être faisable facilement.

Vie privée restaurée

Que l'entreprise stocke les données en interne ou dans le cloud, la conclusion est que la confidentialité et la sécurité des données collectées doivent être maintenues. Les entreprises modèles devraient déjà adhérer à bon nombre des principes énoncés dans le RGPD dans le but de minimiser les risques associés à la vie privée dans le monde d'aujourd'hui. Il est également judicieux d'examiner toutes les données que votre entreprise stocke actuellement auprès de vos clients afin de vous assurer que vous ne recueillez que les données dont vous avez besoin et les données que vous avez indiquées collecter. Les entreprises - en particulier celles qui se trouvent en dehors de l'Europe où les entreprises stockent des données clients à des fins de marketing - devront tenir compte d'une révision des bases de données et de toute donnée de client associée. Lors du développement et de l'utilisation d'applications, de services et de produits qui traitent des données personnelles, un processus d'examen strict pour la collecte et la protection des données devrait toujours être en place. Adopter une approche proactive de la collecte de données du point de vue de l'utilisateur peut également vous aider à répondre aux éventuelles demandes futures des clients souhaitant que leur vie privée soit restaurée en supprimant ces données.

Se préparer pour 2018

En réalité, la plupart des règlements sont loin d'être précis lorsqu'ils tentent de

PRÉPAREZ-VOUS POUR LE RGPD
Règlement Général sur la Protection des Données

définir des normes de conformité et d'établir des exigences de base auprès des organisations et de leurs services informatiques. Comme pour la plupart des réglementations de confidentialité associées, le RGPD exige que les organisations concernées appliquent les meilleures pratiques et mettent en place certains processus de protection afin de mieux protéger les droits à la vie privée et la sécurité des données de leurs clients. Cependant, il ne spécifie pas de solutions de sécurité particulières qui devraient être déployées, par exemple, qui peuvent présenter certains défis pour les départements informatiques. Pourtant, le RGPD exige encore une approche complète de la sécurité de l'information, des pratiques exemplaires exigeantes, une documentation adéquate et des types de protection efficaces. Dans cet esprit, il ne s'agit que de quelques bonnes pratiques. Les organisations devraient envisager maintenant de se préparer au RGPD lorsque le nouveau règlement entrera en jeu en **mai 2018** :

- Effectuer un audit de données pour savoir quelles données vous détenez et comment vous les utiliser
- Classer les données par sensibilité et ne prenez pas en compte les données clients non critiques ou non nécessaires, minimisant ainsi les risques
- L'archivage des e-mails et la sauvegarde des données doivent être surveillés et les règles doivent être appliquées pour éviter les incidents involontaires (et intentionnels)
- Mettre en place des programmes de sensibilisation du personnel et de formation aux utilisateurs pour se concentrer sur la protection des données
- Effectuer un examen en continu pour déterminer et définir exactement quels utilisateurs devraient avoir un accès limité aux données des clients
- Envisager d'utiliser l'authentification à deux facteurs pour tout compte avec un accès aux données sensibles
- Mettre en œuvre une approche de sécurité multi-couches pour les réseaux d'emails et d'entreprise afin d'éviter les attaques de phishing et de ransomware
- Élaborez un plan de réponse à la violation des données afin d'assurer un signalement dans les 72 heures.
- Désignez un agent de protection des données (DPO) si vous êtes une entreprise - conformément aux exigences du RGPD

Comment AppRiver peut aider?

À sa base, la confidentialité par conception (Privacy by design) implique l'inclusion de la protection des données dès le début du développement d'un système, plutôt qu'une addition ultérieure. Plus précisément, conformément à l'exigence du RGPD : «Le contrôleur doit ... mettre en œuvre des mesures techniques et organisationnelles appropriées ... de manière efficace ... afin de satisfaire les exigences du présent règlement et de protéger les droits des personnes concernées». **L'ensemble des solutions avancées de protection contre les menaces et la fonctionnalité de chiffrage par messagerie**

PRÉPAREZ-VOUS POUR LE RGPD
Règlement Général sur la Protection des Données

électronique d'AppRiver permettent aux PME de se protéger contre les violations de sécurité et de données grâce à une approche de sécurité multi-couches de qualité.

Securité et confidentialité "par conception"

La sécurité et la confidentialité "par conception" font partie intégrante de la sécurisation des données de votre client. Dans le cadre d'une exigence légale avec le RGPD, il devient essentiel d'avoir un plan complet en place. La documentation de chaque couche de défense et votre politique de confidentialité permettront à votre organisation de fournir aux clients potentiels et existants une assurance que la protection fournie peut les aider à respecter l'exigence du règlement.

Vérifiez et surveillez votre réseau

Chaque entreprise, y compris la vôtre, possède des actifs informatiques précieux tels que les ordinateurs, les réseaux et les données. La protection de ces actifs exige que les entreprises de toutes tailles effectuent des **audits de sécurité informatique** pour avoir une image claire du statut de leur réseau, des obstacles de sécurité auxquels ils sont confrontés et de la meilleure façon de faire face à ces menaces.

Si vous avez déjà déployé **SecureSurf®** sur votre réseau, il est conseillé d'exécuter une vérification du réseau à l'aide des options du moniteur disponibles et de déployer l'utilisation du réseau et l'analyse des menaces. Cela produira un rapport vous fournissant des informations critiques sur la santé du réseau et répertoriant tout malware trouvé. Si un malware est détecté, **SecureSurf®** bloquera automatiquement la tentative et donnera à vos administrateurs le temps de nettoyer les PC infectés. De plus, assurez-vous de créer une liste principale des actifs de votre entreprise afin que vous puissiez décider de ceux qui nécessitent une protection. Cette liste d'actifs devrait inclure au minimum des PC, des appareils mobiles, des ordinateurs portables, des routeurs, des téléphones VoIP, des PBX IP, des équipements réseaux et des imprimantes.

Sécurité multi-couches

Sécuriser un réseau avec une approche multicouches est une pratique exemplaire. Votre organisation devrait protéger toutes les failles de sécurité en combinant les solutions de sécurité E-mail et Web avec une couche de protection AV Endpoint. Les plates-formes de protection Web telles que **SecureSurf®** complètent **SecureTide®** Email Security et les points d'extrémité AV en bloquant les logiciels malveillants à la source, et analyse les réseaux à la recherche de logiciels malveillants résidents qui n'ont pas été détectés dans le passé et pourraient potentiellement être dangereux. En déployant **la bonne combinaison** de **solutionsSecurity, Network & Web Security et Endpoint AV**, votre entreprise peut mettre un terme aux lacunes de sécurité disponibles dans chaque réseau et obtenir un suivi du trafic entrant et sortant.

PRÉPAREZ-VOUS POUR LE RGPD
Règlement Général sur la Protection des Données

Cryptage des e-mails

Le courrier électronique peut parcourir un long chemin avant qu'il n'atteigne votre boîte de réception. Avec **CipherPost Pro®** d'AppRiver, vous éviterez les regards indiscrets en cours de route. Avec un seul clic, **CipherPost Pro** crypte votre message lorsqu'il quitte votre boîte aux lettres. Seul le destinataire autorisé - avec le mot de passe approprié - peut lire le message. Les données du client restent ainsi privées et protégées en cours de route. Le chiffrement des e-mails de CipherPost Pro vous confère une vraie sécurité de vos boîtes aux lettres, quelle que soit l'emplacement de votre courrier électronique, en veillant à ce que la confidentialité des données soit maintenue. CipherPost Pro® vous aidera à remplir la «responsabilité» exigée à l'article 5: 2 du RGPD. Vous pouvez utiliser en complément l'option de bordereau de livraison pour vérifier et contrôler l'état de tous vos emails cryptés à tout moment.

Solutions associées

SecureTide® – *Spam and Virus Protection - Protection contre les spams et les virus*
SecureSurf® – *Web & Network Protection - Protection réseaux et web*
CipherPost Pro® – *Email Encryption - Cryptage d'e-mails*


appriver