VEEAM

RGPD : 5 leçons apprises L'expérience de Veeam en matière de conformité

Synthèse DSI

Mark Wong
Directeur juridique

Introduction

L'objet de ce livre blanc est de vous faire découvrir ce que le RGPD signifie pour Veeam. Les informations relatives au RGPD abondent sur l'internet et, si de nombre d'entreprises et d'avocats peuvent se positionner en tant qu'experts, la conformité au RGPD est spécifique à chaque entreprise. Vous connaissez votre entreprise mieux que quiconque. C'est donc vous qui êtes en meilleure position pour devenir son véritable expert en matière de conformité au RGPD. Nous partagerons nos perspectives et les leçons que nous avons apprises dans notre propre démarche de conformité. Elles vous aideront dans votre réflexion non seulement sur la conformité au RGPD, mais aussi sur la manière dont les solutions logicielles de Veeam peuvent jouer un rôle critique dans vos stratégies d'administration et de protection des données et assurer que votre entreprise est Always-On™.

Ce livre blanc est destiné à être plus technique et nous aborderons et expliquerons notre vision du RGPD du point de vue de la conformité technique et juridique. Nous examinerons les principes qui sous-tendent le RGPD et la manière dont le RGPD a évolué en loi de référence régissant la confidentialité des données en Europe depuis la Directive de protection des données de 1995 qu'elle remplace. Le changement le plus notable apporté par le RGPD consiste à redonner le contrôle des données personnelles aux individus. Les entreprises qui recueillent, traitent, analysent et utilisent ces données personnelles ont plus d'obligations vis-à-vis de ces individus. La confidentialité des données est un des droits fondamentaux de l'individu. Toute entreprise qui manipule des données personnelles doit s'assurer de faire un usage légal de ces données et les protéger au même niveau que ses informations confidentielles. Nous croyons que nos produits et nos solutions peuvent aider votre entreprise à assurer la disponibilité de votre Always-On Enterprise.

Quand le RGPD entre-t-il en vigueur ?

Le 25 mai 2018. Le RGPD est devenu une loi à part entière le 27 avril 2016, mais prévoyait une période de deux ans pour permettre aux entreprises d'effectuer la transition de la Directive de protection des données aux exigences plus nombreuses du RGPD.

En réalité, que demande le RGPD aux entreprises ?

Le RGPD s'articule autour de cinq principes fondamentaux.

1. **Connaître vos données.** Identifiez les informations d'identification personnelle (PII) que votre entreprise recueille et les individus qui y ont accès.
2. **Administrer vos données.** Établissez les règles et les procédures d'accès et d'utilisation des PII.
3. **Protéger vos données.** Implémentez et assurez la mise en place de contrôles de sécurité pour protéger les informations et répondre aux violations de données.
4. **Documenter et être conforme.** Documentez vos processus, exécutez les demandes concernant les données et signalez tous les problèmes ou violations de données dans le cadre des directives.
5. **Amélioration continue.** Notre monde numérique évolue de manière permanente et Veeam estime qu'il changera plus au cours des cinq prochaines années qu'il ne l'a fait pendant les dix dernières années. Les entreprises doivent constamment évaluer et tester leurs procédures et protocoles existants pour les faire évoluer et les améliorer au rythme des changements de notre monde numérique.

Pourquoi n'existe-t-il pas une solution universelle à la conformité RGPD ?

Bien que la loi soit la même, les entreprises qui doivent s'y conformer sont uniques et la manière dont elles recueillent, gèrent, utilisent et protègent les données est différente. Les PII sont également différentes car il s'agit d'informations diversifiées généralement définies comme toutes les données qui peuvent être utilisées pour identifier un individu. Cela comprend les identificateurs en ligne (adresses IP), le nom, les informations de contact, les bases de données commerciales, les données de support client, les commentaires des clients, les données de géolocalisation, les séquences vidéo, les programmes de fidélisation, les informations médicales et financières ainsi que d'autres. Il existe aussi une catégorie de PII critiques comprenant la race, l'origine ethnique, les bilans de santé et l'orientation sexuelle. Les directives qui s'adressent aux processeurs de ce type de PII critiques sont encore plus strictes que celles concernant les PII « ordinaires ». Alors que de nombreuses entreprises se trouvent confrontées à des situations similaires, les différences vont venir du volume, du type, de l'objet et surtout des gens. Un des aspects critiques de la conformité au RGPD est de former les collaborateurs au traitement des PII.

Quels sont les changements prévus par la nouvelle réglementation ?

Le RGPD a été promulgué pour mettre en œuvre un large éventail d'obligations dans les entreprises qui recueillent ou traitent des PII. Les objectifs et les principes du RGPD sont les suivants :

1. **Offrir équité et transparence aux individus.** Les entreprises doivent informer les individus de la manière dont leurs PII sont utilisées dans un but légal.
2. **Limiter l'utilisation au nécessaire.** Les entreprises peuvent utiliser les PII uniquement à des fins précises, spécifiées et légitimes. Les PII peuvent être utilisées uniquement pour les raisons ou les buts communiqués à l'individu.
3. **Recueillir uniquement ce dont on a besoin.** Il existe une large palette de PII et une entreprise ne doit recueillir que les PII nécessaires et appropriées à son but.
4. **Exactitude et droit à l'oubli.** Les entreprises ont désormais la responsabilité de maintenir des enregistrements exacts et doivent exécuter les demandes de correction de PII formulées par l'individu auquel elles se rapportent. Les entreprises doivent également respecter le désir d'un individu d'être oublié, ce qui signifie que l'entreprise doit effacer les PII dans la mesure du possible.
5. **Limiter le stockage** Les PII doivent être stockées uniquement pour la durée nécessaire à la réalisation du but précis et légitime énoncé.
6. **Sécuriser les données.** Les entreprises doivent prendre des mesures pour sécuriser les PII au moyen de procédures et de techniques telles que le chiffrement logiciel.
7. **Désigner un délégué à la protection des données.** La création de ce poste sera exigée pour la supervision à grande échelle des données. Le délégué à la protection des données devra maîtriser la loi et les pratiques de protection des données et rendra directement compte au sommet de la hiérarchie.

Qui doit être conforme au RGPD ?

Les entreprises de l'UE qui traitent des PII et toute entreprise hors de l'UE qui traite des PII de résidents européens dans le but d'offrir des services, des marchandises ou d'analyser leur comportement (réseaux sociaux par exemple). Il y a un grand changement par rapport à la Directive de protection des données qui ne s'appliquait qu'aux « contrôleurs », à savoir ceux qui recueillaient et traitaient les données eux-mêmes. Le RGPD s'applique également aux « processeurs », à savoir les entreprises qui traitent les PII pour le compte de tiers.

Quelles sont les amendes ?

Une des différences majeures entre le RGPD et la Directive de protection des données, ce sont les amendes importantes qui peuvent être infligées dans le cadre du RGPD. L'amende maximale est la somme la plus élevée entre 4 % du CA mondial de votre entreprise ou 20 millions d'euros. Remarquez qu'il s'agit là d'une amende maximale et que son montant variera en fonction de la sévérité des violations.

Quel est le cadre légal du traitement des PII ?

Il existe plusieurs motifs fournis par le RGPD, y compris le traitement d'informations nécessaires à l'exécution d'un contrat. L'individu consent au traitement de ses PII si une entreprise a un intérêt légitime et véritable qui l'emporte sur son droit à la confidentialité.

Quelle est la différence entre les méthodes de sécurité organisationnelles et techniques ?

Le RGPD aborde aussi bien les méthodes organisationnelles que les méthodes techniques pour assurer la sécurité des PII. Selon le RGPD, les méthodes de sécurité organisationnelles peuvent consister à limiter le nombre de collaborateurs de votre entreprise qui ont accès aux PII. Les méthodes techniques peuvent mettre en jeu des mots de passe spécifiques pour l'accès aux PII ou le chiffrement. Le RGPD laisse aux entreprises toute latitude pour déterminer la combinaison de mesures de sécurité suffisante pour protéger les PII concernées.

Quel type de journalisation le RGPD exige-t-il ?

Le RGPD exige des audits, des procédures et des processus améliorés pour protéger les PII. Les entreprises sont tenues de conserver des enregistrements de leurs activités de traitement des données et en particulier des transferts de PII à l'extérieur de l'UE. Il est indispensable de documenter les mesures de sécurité prises. Même s'il existe de nombreux fournisseurs offrant des conseils dans ce domaine, les entreprises sont elles-mêmes responsables de l'exécution des évaluations.

Puis-je transférer des PII à l'extérieur de l'UE ?

Oui, mais le RGPD est très strict en ce qui concerne le transfert de PII de résidents européens en dehors de l'UE. Il existe certains mécanismes tels que les contrats ou les certifications qui permettent ces transferts.

Qu'en est-il de mes fournisseurs et partenaires qui peuvent avoir accès aux PII que mon entreprise a recueillies ?

Les processeurs du RGPD doivent garantir aux contrôleurs que les mesures de sécurité techniques et organisationnelles appropriées sont prises pour recevoir et traiter les PII. Si votre entreprise est en relation avec des fournisseurs et des tierces parties utilisant les PII que votre entreprise a recueillies, assurez-vous qu'ils sont également conformes au RGPD et garantissent que vous l'êtes aussi.

Le RGPD en bref :

- Le RGPD donne aux individus le pouvoir de contrôler leurs PII. Les entreprises doivent informer les individus des buts dans lesquels elles traitent leurs PII.
- Les individus ont le droit de demander la correction ou la suppression de leurs PII et de demander à ce qu'elles ne soient plus traitées (opt out).
- Les individus ont droit à la portabilité des données et les entreprises doivent leur fournir assistance s'ils en font la demande.
- La conformité au RGPD ne s'arrête pas le 25 mai 2018. C'est un processus d'administration, de supervision et d'amélioration constantes.

Pour en savoir plus sur la démarche de conformité du RGPD de Veeam et les cinq principes clés, téléchargez ce guide étape par étape destiné aux professionnels de l'informatique : https://www.veeam.com/wp-gdpr-compliance-experience.html

Veeam® s'engage à vous faire part de son expérience du Règlement général sur la protection des données (RGPD). Cette réglementation est complexe et spécifique à chaque entreprise et la conformité au RGPD peut avoir un sens différent d'une entreprise à l'autre. Le RGPD est une mise à jour majeure de la Directive de protection des données de 1995 (ou plus spécifiquement 95/46/EC) et les grands volumes de données d'aujourd'hui sont très différents de ceux de 1995.

Beaucoup pourraient penser que le RGPD est simplement un problème informatique, mais rien n'est plus loin de la vérité. Il touche tout le monde — et pas seulement l'IT.

Nous avons préparé ce livre blanc pour aborder la manière dont Veeam interprète le RGPD à la date de publication. Nous sommes une société privée de technologies de l'information qui développe des logiciels de sauvegarde, de reprise après incident et d'administration des données pour les workloads virtuels, physiques et cloud afin d'assurer l'Availability for the Always-On Enterprise™. Nous avons consacré beaucoup de temps au RGPD, non seulement dans le cadre de notre démarche de conformité d'entreprise internationale, mais aussi dans le développement de nos produits.

Ce livre blanc ne se substitue pas à un conseil juridique et ne permet pas de déterminer comment le RGPD s'applique à votre entreprise. Nous vous encourageons à faire comme nous et à collaborer avec des professionnels qualifiés pour discuter du RGPD et de la manière dont il s'applique à votre entreprise et pour concevoir un plan de mise en conformité. Veeam fournit ce livre blanc « tel quel » et n'offre aucune garantie expresse ou implicite quant aux informations contenues dans le présent livre blanc.

Publié en janvier 2018. Version 1.0

À propos de Veeam Software

Veeam® connaît les nouveaux défis que rencontrent les entreprises du monde entier pour assurer l'Always-On Enterprise™ et garantir une activité ininterrompue 24.7.365. Pour y répondre, Veeam a créé le marché de l'Availability for the Always-On Enterprise™ en aidant les entreprises à atteindre des temps de restauration et des délais optimaux de reprise d'activité (RTPO™) inférieurs à 15 minutes pour toutes les applications et toutes les données au moyen d'un type de solution fondamentalement nouveau qui offre une restauration ultrarapide, la prévention contre la perte de données, une vérification des capacités de restauration, une mise à profit des données et une visibilité complète. Veeam Availability Suite™ comprend Veeam Backup & Replication™ et tire parti des technologies de virtualisation, de stockage et de cloud du datacenter moderne pour aider les entreprises à gagner du temps, minimiser les risques et réduire leurs coûts d'investissement et d'exploitation de manière significative.

Fondée en 2006, Veeam Software compte actuellement 51 000 revendeurs ProPartner et plus de 282 000 clients dans le monde entier. Le siège social de Veeam se trouve à Baar, en Suisse, et la société possède des filiales dans le monde entier. Pour en savoir plus, visitez http://www.veeam.com/fr.

VEEAM EST TRÈS FIER DE NOS

1 MILLION
D'UTILISATEURS

51 000
PARTENAIRES

282 000
CLIENTS

80
RÉCOMPENSES MAJEURES

PARTENAIRES GLOBAL ALLIANCE

Cisco Preferred Solution Partner

DELL EMC

Hewlett Packard Enterprise

Gold Microsoft Partner

NetApp ALLIANCE PARTNER

vmware PARTNER TECHNOLOGY ALLIANCE

RESTEZ CONNECTÉ

VeeamSoftware

@veeam_software

@Veeam

Veeam Software

Veeam

www.veeam.com/fr