RGPD : 5 leçons apprises

L'expérience de Veeam en matière de conformité

Le 25 mai 2018
LE RGPD ENTRERA EN VIGUEUR
SOYEZ CONFORME

Le Règlement général sur la protection des données (RGPD) oblige les entreprises à protéger les données personnelles et la confidentialité des citoyens européens dans les transactions effectuées dans les états membres de l'UE. Vous devez être capable de garantir la sécurité de toutes les données personnelles que vous recueillez et/ou traitez — ou subir éventuellement des sanctions.

Découvrez les cinq leçons essentielles apprises par Veeam® au cours de notre démarche de conformité et accélérez vos initiatives RGPD. Il n'est pas trop tard !

La conformité au RGPD ne peut pas être atteinte en utilisant une seule solution

Le RGPD englobe toutes les strates de l'entreprise, y compris la sensibilisation des collaborateurs, les processus métier et de gouvernance, la supervision et le reporting ainsi que les systèmes d'information.

Sanctions pour non-conformité de 4 % du CA annuel mondial ou 20 millions d'euros

Concerne les entreprises traitant des données personnelles de résidents de l'UE

Des délégués à la protection des données (DPO/DPD) peuvent être requis

Notifier les autorités et les individus concernés d'une violation dans des délais restreints

Le consentement doit être clair, mis en évidence et inclure les raisons du recueil des informations

Les personnes concernées peuvent décider de révoquer l'accès à leurs données

Les personnes concernées ont le droit d'obtenir, de modifier, de déplacer et de supprimer leurs données

Prévoir la protection des données dès la phase de conception d'un nouveau système

En réalité, que demande le RGPD aux entreprises ? Cinq leçons essentielles apprises par Veeam :

1. **Connaissez vos données** — Identifiez les informations d'identification personnelle (PII) que votre entreprise recueille et les individus qui y ont accès.
2. **Administrez vos données** — Établissez les règles et les procédures d'accès et d'utilisation des PII.
3. **Protégez vos données** — Implémentez et assurez la mise en place de contrôles de sécurité pour protéger les informations et réagir en cas de violation de données.
4. **Documentez et soyez 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. **Examinez et améliorez constamment** vos processus et vos procédures de confidentialité et de protection des données.

Veeam Availability Suite offre des informations approfondies sur la protection, l'audit et le reporting des données au moyen de fonctionnalités adaptées aux grandes entreprises pour vous assister dans votre démarche de conformité au RGPD.

Articles du RGPD de l'UE relatifs à l'administration des données et contexte Veeam	Article 5 — Principes relatifs au traitement des données à caractère personnel Article 6 — Licéité du traitement Article 9 — Traitement portant sur des catégories particulières de données à caractère personnel Article 15 — Droit d'accès de la personne concernée Article 17 — Droit à l'effacement (« droit à l'oubli ») Article 20 — Droit à la portabilité des données Article 25 — Protection des données dès la conception et protection des données par défaut Article 30 — Registre des activités de traitement Article 32 — Sécurité du traitement Article 35 — Analyse d'impact relative à la protection des données Article 39 — Missions du délégué à la protection des données Article 44 — Principe général applicable aux transferts
Disponibilité de vos données	L'article 32 du RGPD explique que vous devez rétablir la disponibilité des données en cas de catastrophe, d'attaque de logiciel malveillant (ransomware) ou d'autre problème. Grâce à Instant VM Recovery®, vous pouvez rapidement rétablir la disponibilité de vos données et Veeam Backup & Replication™ offre plus de 50 possibilités de restauration pour chaque sauvegarde. L'article 20 du RGPD exige que vous rendiez à une personne les données qui la concernent en votre possession. Les capacités avancées de restauration de Veeam vous donnent la possibilité d'explorer les sauvegardes et les réplicas et de restaurer les données dans des formats courants afin de livrer les données aux personnes concernées en temps voulu.
Taguage des PII et analyses	Lorsque des données de type PII sont identifiées, il est essentiel de les superviser et de les auditer avec une diligence constante. Avec Veeam ONE™, vous pouvez taguer les sources de votre infrastructure contenant des PII et exécuter des rapports, examiner des tableaux de bord et effectuer l'audit de certaines activités (par ex., ce qui est restauré et qui effectue les restaurations) survenant dans votre environnement. Ce sont des parties importantes des articles 6, 32 et 35 du RGPD, y compris pour le délégué à la protection des données dont la mission est décrite à l'article 39 du RGPD.
Rétention des données et droit à l'oubli	Bien que le droit à l'oubli (article 17 du RGPD) ne soit pas absolu, vous ne pouvez pas conserver les données plus longtemps que juridiquement nécessaire (selon les lois de chaque pays et les segments verticaux). Pour ce qui est de la rétention des données, vous pouvez clairement marquer les sauvegardes comme périmées et Veeam Backup & Replication supprimera les points de rétention des données lorsque le délai sera écoulé. Ceci est décrit à l'article 6 du RGPD.
Exploration des données	Une des premières tâches que toute entreprise doit effectuer dans sa démarche de conformité au RGPD est de déterminer les données qu'elle possède. L'analyse des sources de données n'est pas toujours facile en production. Veeam Availability Suite™ et la technologie Veeam Explorer™, l'indexation des fichiers invités et les Virtual Labs donnent à votre entreprise la capacité d'explorer les données qui résident dans vos copies.
SureBackup, SureReplica et Virtual Labs	SureBackup et SureReplica sont destinés à automatiser et simplifier les processus de vérification des sauvegardes. C'est la partie la plus cruciale de l'administration et de la protection des données pour assurer la protection des données des personnes au titre des articles 5 et 25 du RGPD. Vous pouvez vérifier automatiquement chaque point de restauration dans chaque VM ou réplica et vous assurer qu'ils fonctionnent comme prévu au cas où vous seriez dans l'obligation d'utiliser ou de générer des rapports sur ces inestimables points de restauration. Cela donne à l'équipe qui sous-traite vos données les outils nécessaires pour se conformer aux divers aspects du RGPD de manière transparente. Les Virtual Labs constituant la technologie sous-jacente peuvent être utilisés pour réaliser des évaluations d'impact sur la protection des données avant d'effectuer des mises à jour, mises à niveau ou opérations de maintenance sur vos données de production, ce qui est un point essentiel de l'article 35 du RGPD.
Rapports d'emplacement	Il est essentiel de pouvoir protéger et chiffrer les données au fil de leurs déplacements dans votre entreprise et vers l'extérieur. Cependant, il est également nécessaire de déterminer exactement et de documenter l'emplacement géographique et l'état de ces enregistrements de données sur les personnes. Cela s'applique à vos données de production, mais aussi à toutes les copies de ces données. Avec Veeam Availability Suite 9.5 Update 3, vous pouvez taguer l'emplacement de chaque point de données et générer des rapports sur toutes les données de production et leurs sauvegardes, copies de ces sauvegardes, bandes et réplicas, leur emplacement géographique et les éventuelles disparités entre emplacements. Ceci est vital pour maintenir la conformité aux articles 15 et 44 du RGPD.
Chiffrement de bout en bout	L'article 44 du RGPD fait référence aux transferts de données entre régions ou pays dans et hors de l'Union européenne. Pendant ces processus, il est essentiel de transmettre les informations sur les personnes au moyen de canaux chiffrés et sécurisés. Veeam offre un chiffrement intégré AES 256 bits de bout en bout et vous donne la possibilité de chiffrer vos fichiers et vos données de sauvegarde à la source (pendant la sauvegarde), en cours de transfert et au repos. Ceci est primordial pour assurer la conformité aux articles 32 et 44 du RGPD dans l'ensemble de votre entreprise et de ses filiales ou entités associées.
Contrôles d'accès basé sur les rôles	De nombreux articles du RGPD mentionnent la journalisation des activités, la documentation de ces activités et la définition de ceux qui ont accès à quelles données. Veeam Availability Suite comporte des contrôles RBAC intégrés pour vous permettre de restreindre les accès à certains points de données de votre environnement. Avec Veeam Backup Enterprise Manager, un composant de Veeam Availability Suite, vous pouvez aussi autoriser vos utilisateurs finaux à effectuer des opérations en libre-service, limiter leur accès à certaines données ou leur donner accès uniquement lorsque cela est nécessaire dans le cadre de leurs responsabilités.
Exclusion de données	Certaines données doivent être traitées de manière particulière (ou même exclues — article 9 du RGPD) et la journalisation de ces traitements doit être effectuée (article 30 du RGPD). En utilisant les exclusions de Veeam Availability Suite, vous pouvez facilement exclure les données en fonction de VMs, de disques et même de fichiers ou de dossiers spécifiques au moyen d'agents et assurer ainsi votre conformité.