GDPR: 5 lições aprendidas

Experiência de conformidade da Veeam compartilhada

25 de maio de 2018
O GDPR VAI ENTRAR EM VIGOR
ESTEJA EM CONFORMIDADE JÁ

O Regulamento Geral de Proteção de Dados (GDPR) exige que as empresas protejam os dados pessoais e a privacidade de cidadãos da UE em relação a transações que ocorram dentro dos estados integrantes da UE. Você deve ser capaz de garantir a segurança de todos os dados pessoais que você coleta e/ou processa, ou possivelmente enfrentará multas.

Descubra as cinco principais lições aprendidas pela Veeam® em nossa jornada rumo à conformidade com GDPR e impulsione suas iniciativas com GDPR. Ainda dá tempo!

A conformidade com GDPR não pode ser alcançada utilizando uma única solução

O GDPR abrange todas as camadas de uma empresa, incluindo conscientização de funcionários, processos de negócios e de governança, monitoramento e relatórios e sistemas de informação.

Multas por não conformidade de 4% do Lucro Anual Global ou 20 milhões de euros

Efeito de empresas que processam dados pessoais de pessoas na UE

Escritórios de Proteção de Dados (DPO) podem ser exigidos

Notificar autoridades e indivíduos de uma violação dentro prazos curtos

O consentimento deve se destacar, ser claro e incluir os motivos da coleta

As pessoas podem decidir revogar o acesso dos seus dados

As pessoas têm o direito de obter, alterar, mover ou excluir seus dados

Incluir proteção de dados na fase de projeto de um sistema novo

O que o GDPR realmente exige das organizações? Cinco lições fundamentais aprendidas pela Veeam

1. **Conheça seus dados —** Identifique as Informações de Identificação Pessoal (PII) que a sua empresa coleta e quem tem acesso a elas.
2. **Gerencie seus dados** — Estabeleça regras e procedimentos para o acesso e uso de PII.
3. **Proteja seus dados** — Implemente e certifique-se de que os controles de segurança estão aptos para proteger informações e responder a violações de dados.
4. **Documentação e conformidade** — Documente seus processos, execute solicitações de dados e relate qualquer problema ou violação de dados nas diretrizes.
5. **Analise e melhore constantemente** seus processos e procedimentos para proteção e privacidade de dados.

O Veeam Availability Suite fornece insights detalhados de proteção de dados, auditorias e relatórios com recursos de nível corporativo para lhe ajudar na jornada rumo à conformidade com GDPR.

Artigos de GDPR da UE sobre gerenciamento de dados e a estrutura Veeam	Artigo 5 — Princípios relacionados ao processamento de dados pessoais Artigo 6 — Legitimidade do processamento Artigo 9 — Processamento de categorias especiais de dados pessoais Artigo 15 — Direito de acesso pelo titular dos dados Artigo 17 — Direito à exclusão (direito de ser esquecido) Artigo 20 — Direito à portabilidade de dados Artigo 25 — Proteção de dados por concepção e por padrão Artigo 30 — Registros de atividades de processamento Artigo 32 — Segurança do processamento Artigo 35 — Avaliação de impacto da proteção de dados Artigo 39 — Tarefas do responsável pela proteção de dados Artigo 44 — Princípio geral para transferências
Disponibilidade dos seus dados	O artigo 32 do GDPR explica que você precisa tornar os dados disponíveis novamente em caso de um desastre, ataque de malware (ransomware) ou outros problemas. Com o Instant VM Recovery®, você pode tornar os dados disponíveis novamente de maneira rápida, e o Veeam Backup & Replication™ possui mais de 50 possibilidades de recuperação em um único backup. O artigo 20 do GDPR exige que você devolva os dados que possui de algum indivíduo para ele ou ela. Os recursos de recuperação avançados da Veeam lhe fornecem a possibilidade de explorar backups e réplicas, e recuperar os dados em formatos comuns, permitindo enviá-los aos titulares antecipadamente.
Identificação de dados PII e análises	Quando dados PII são identificados, é crucial monitorar e fiscalizar com cuidado constante. Com o Veeam ONE™, você pode identificar as bases da sua infraestrutura caso elas tenham PII e executar relatórios nelas, examinar painéis e realizar auditorias sobre determinadas atividades (por exemplo, o que é restaurado e quem realizou as restaurações) no seu ambiente. São partes importantes dos artigos 6, 32 e 35 do GDPR, e também para que o responsável pela proteção de dados realize seus deveres do artigo 39 do GDPR.
Retenção de dados e o direito de ser esquecido	Embora o direito de ser esquecido (artigo 17 do GDPR) não seja absoluto, você não pode manter os dados por mais tempo do que seja legalmente necessário (dependendo das leis do país e dos segmentos verticais). Com a retenção de dados, você pode marcar backups obsoletos e o Veeam Backup & Replication removerá os pontos de retenção de dados quando a retenção for aprovada, descrita no artigo 6 da GDPR.
Descoberta de dados	Uma das primeiras tarefas que uma organização precisa fazer na sua jornada à conformidade com GDPR é descobrir quais dados possui. Investigar as fontes de dados na produção nem sempre é fácil. O Veeam Availability Suite™ e a tecnologia do Veeam Explorer™, indexação de arquivos guest e Virtual Labs, fornecem à sua organização a capacidade de realizar descobertas de dados que residem nas cópias.
SureBackup, SureReplica e Virtual Labs	O SureBackup e o SureReplica são destinados à automação e facilitação dos processos de verificação de backup. Essa é a parte mais importante do gerenciamento e proteção de dados ao aderir a proteção de dados privados de indivíduos nos artigos 5 e 25 do GDPR. Você pode verificar automaticamente cada ponto de restauração criado de cada VM ou réplica e garantir que eles funcionarão caso seja requerido que você resgate ou relate sobre esses pontos de restauração de grande valor. Isso oferece à sua equipe de processamento de dados as ferramentas necessárias para conformidade com vários elementos do GDPR de maneira coesa. O Virtual Labs, que é a tecnologia subjacente, pode ser usado para realizar avaliações de impacto de proteção de dados antes de executar atualizações, melhorias ou manutenções nos seus dados de produção, que é um item fundamental do artigo 35 do GDPR.
Relatórios de localização	Com um fluxo pesado de dados na sua organização, é essencial ser capaz de proteger e criptografar. Porém, também é necessário localizar e relatar a localização geográfica e o estado desses registros de dados de indivíduos. Isso se aplica aos seus dados de produção e também a todas as cópias desses dados. Com o Veeam Availability Suite 9.5 Update 3, você poderá identificar a localização de cada ponto de dados e reportar todos os dados de produção e backups relevantes, cópias de backup, fitas e réplicas, suas localizações geográficas e qualquer incompatibilidade entre os locais. Isso é vital para manter a integridade do artigo 15 e 44 do GDPR.
Criptografia de ponta a ponta	O artigo 44 do GDPR é referente a transferências de dados entre regiões ou localizações internacionais dentro e fora da União Europeia. Durante esses processos, é crucial transmitir as informações de dados de indivíduos utilizando canais seguros de criptografia. A Veeam fornece criptografia integrada AES de 256 bits de ponta a ponta, dando a você a capacidade de criptografar arquivos de backup e dados na origem (durante o backup), em transmissão e em repouso. Isso é indispensável para que toda a sua organização, órgãos ou associações afiliadas estejam em conformidade com os artigos 32 e 44 do GDPR.
Controles de acesso baseados em funções	Muitos artigos do GDPR falam sobre registros de atividades, reportar essas atividades e definir quem tem acesso a qual dado. O Veeam Availability Suite possui controles RBAC (controle de acesso baseado em função) integrados que permitem restringir o acesso a determinados pontos de dados do seu ambiente. Com o Veeam Backup Enterprise Manager, parte do Veeam Availability Suite, você também pode permitir autosserviço para seus usuários finais e limitar ou permitir acesso a dados específicos quando forem necessários para o cumprimento de responsabilidades.
Exclusão de dados	Alguns dados devem ser processados expressamente (ou até excluídos — artigo 9 do GDPR) e os registros desse processamento devem ser mantidos (artigo 30 do GDPR). Ao utilizar exclusões no Veeam Availability Suite, você pode facilmente excluir dados baseados em VMs, discos e até de arquivos/pastas com agentes, mantendo-se em conformidade.