GDPR: Öğrenilecek 5 Ders

Veeam uyumluluk için deneyimini paylaşıyor

25 Mayıs 2018
GDPR YÜRÜRLÜĞE GİRECEK
HAZIR OLUN

Genel Veri Koruma Düzenlemesi (GDPR) işletmelerin, AB vatandaşlarının AB üyesi ülkeler içerisinde gerçekleştirecekleri işlemlerdeki kişisel verilerini ve gizliliğini korumasını gerektirir. Topladığınız ve/veya işlediğiniz kişisel verilerin güvenliğini garanti edebilmelisiniz; yoksa cezaya çarptırılabilirsiniz.

Veeam®'in GDPR uyumluluğu yolunda öğrendiği beş önemli dersi keşfedin ve GDPR süreçlerinize hız kazandırın. Henüz çok geç değil!

GDPR uyumluluğu tek bir çözüm kullanarak sağlanamaz

GDPR bir şirketin çalışan farkındalığı, iş ve yönetim süreçleri, izleme ve raporlama ile bilgi sistemleri de dahil olmak üzere tüm katmanlarını kapsar.

Uyumluluk gerekliliğinin yerine getirilmediği durumlarda Yıllık Global Ciro'nun %4'ü kadar veya 20 Milyon Euro uyumsuzluk cezası	AB'de bireylerin kişisel verilerini işleyen şirketlerin etkisi	Veri Koruma Ofisleri (DPO) gerekli olabilir	Yetkilileri ve bireyleri olası bir ihlal durumunda belirlenen süre içerisinde kesinlikle haberdar edin
Onay belgesi ön planda ve net olmalı ve veri toplama nedenlerini de içermelidir	Kişiler verilerine erişim izninizi kaldırmaya karar verebilir	Kişiler kendilerine ait verileri elde etme, değiştirme, taşıma ve silme hakkına sahiptir	Yeni bir sistemde veri korumayı tasarlama aşamasında dahil edin

GDPR kuruluşlardan ne ister? Veeam'in aldığı beş temel ders:

1. **Verilerinizi tanıyın** - Kuruluşunuzun topladığı ve sahip olduğu kişisel olarak tanımlanabilir bilgileri (PII) ve bu bilgilere kimlerin erişebildiğini tanımlayın.
2. **Verileri yönetin** - Kişisel olarak tanımlanabilir bilgilere (PII) ulaşmak ve bu bilgileri kullanmak için uyulması gereken kuralları ve izlenecek süreci belirleyin.
3. **Verileri koruyun** - Bilgileri korumak ve veri ihlallerine karşılık vermek için güvenlik kontrolleri uygulayın ve bu kontrollerin ihlallere karşılık vermeye hazır olduğundan emin olun.
4. **Belgeleyin ve uyumlu olun** - Süreçlerinizi belgeleyin, veri taleplerine göre yürütün ve ortaya çıkacak tüm sorunları veya veri ihlallerini talimatnameye uygun olarak rapor edin.
5. **Süreçlerinizi ve prosedürlerinizi sürekli olarak gözden geçirip geliştirerek** veri gizliliğini ve korumasını sağlayın.

Veeam Availability Suite, GDPR'ye uyumluluk yolculuğunuzda size yardımcı olmak için kuruluş seviyesinde özellikleriyle veri korumaya, denetimine ve rapor etmeye yönelik derinlemesine öngörüler sağlar.

Veri yönetimi hakkındaki AB GDPR maddeleri ve Veeam altyapısı	Madde 5 - Kişisel verilerin işlenmesiyle ilgili ilkeler Madde 6 - İşlemenin yasallığı Madde 9 - Kişisel verilerin özel kategorilerinin işlenmesi Madde 15 - Veri sahibi tarafından verilen erişim hakkı Madde 17 - Silme hakkı (unutulma hakkı) Madde 20 - Veri taşıyabilme hakkı Madde 25 - Tasarım gereği ve varsayılan olarak veri koruma Madde 30 - Etkinlik işleme kayıtları Madde 32 - İşleme güvenliği Madde 35 - Veri koruma etkisi değerlendirmesi Madde 39 - Veri koruma görevlisinin görevleri Madde 44 - Genel aktarım ilkesi
Verilerinizin kesintisiz çalışırlığı	GDPR'nin 32. maddesi uyarınca olası bir felaketin, kötü amaçlı yazılım (fidye yazılım) saldırıların veya diğer problemlerin ortaya çıkması durumunda verileri tekrar çalışır hale getirmeniz gerekir. Instant VM Recovery® ile verilerinizi hızlı bir biçimde tekrar çalışır hale getirebilirsiniz. Ayrıca, Veeam Backup & ReplicationTM sayesinde tek yedeklemede 50'den fazla kurtarma seçeneğine sahip olursunuz. GDPR'nin 20. maddesi uyarınca bulundurduğunuz verileri asıl sahibine iade etmeniz gerekir. Veeam'in gelişmiş kurtarma yetenekleri sayesinde yedekleri ve replikaları inceleme imkanına sahip olursunuz ve verileri ortak formatta kurtararak verileri sahiplerine zamanında teslim edebilirsiniz.
Kişisel olarak tanımlanabilir bilgilerin ve analizlerin etiketlenmesi	Kişisel olarak tanımlanabilir bilgi verileri tanımlanırken tedbir amaçlı olarak sürekli izleme ve denetim yapmak oldukça önemlidir. Veeam ONETM ile altyapı kaynaklarınızda kişisel olarak tanımlanabilir bilgiler bulunuyorsa bu kaynakları etiketleyebilir ve bunlar hakkında rapor hazırlayabilirsiniz. Ayrıca, ortamınızdaki panelleri gözden geçirebilir ve bazı etkinlikleri (örn. neyin kurtarıldığını ve bu kurtarmayı kimin yaptığını) denetleyebilirsiniz. İşte bunlar GDPR'nin 6, 32 ve 35. maddelerinin önemli kısımlarıdır. Ayrıca bu bölüm veri koruma görevlisinin 39. maddede belirtilen görevlerini yerine getirebilmesi için gerekli öğeleri anlatır.
Veri saklama ve unutulma hakkı	Her ne kadar unutulma hakkı (GDPR'nin 17. maddesi) mutlak olmasa da verileri yasal olarak gerekenden (her ülkenin kendi yasalarına ve dikey segmentlerine göre değişiklik gösterebilir) daha fazla tutamazsınız. Veri saklama ile yedeklemeleri kullanımdan kalkmış olarak işaretleyebilirsiniz. Saklama süresi GDPR'nin 6. maddesinde belirtilen süreyi geçtiğinde Veeam Backup & Replication, veri saklama noktalarını kaldıracaktır.
Veri keşfi	Bir kuruluşun GDPR'ye uyumluluk yolculuğunda yapması gereken ilk şeylerden biri hangi verilere sahip olduğunu keşfetmektir. Üretim sırasında veri kaynaklarını soruşturmak her zaman kolay değildir. Veeam ExplorerTM teknolojisine, konuk dosya dizini oluşturma ve Virtual Labs ile birlikte Veeam Availability SuiteTM, kuruluşunuza kopyalarınızda tutulan verileri keşfetme yeteneği sağlar.
SureBackup, SureReplica ve Virtual Labs	SureBackup ve SureReplica yedek doğrulama sürecini otomatikleştirmeyi ve basitleştirmeyi amaçlar. Bu, GDPR'nin 5 ve 25. maddelerindeki kişilere ait özel verilerin korunması ilkesine bağlı kalırken veri yönetimi ve korumasının en önemli bölümüdür. Sanal makine veya replikalar için oluşturulan kurtarma noktalarının tamamını otomatik olarak doğrulayabilir ve bu önemli noktaları kurtarmanız veya bunlar hakkında rapor hazırlamanız gerektiğinde bu noktaların beklediğiniz gibi çalışacağından emin olabilirsiniz. Bu da, veri işleme ekibinizin GDPR çerçevesindeki çeşitli öğelerle sorunsuz bir yöntemle uyumluluk sağlamak için gerekli araçlara sahip olmasını sağlar. Uyumluluğun temelinde yatan teknoloji olan Virtual Labs, üretim verinize güncelleme, yükseltme ve bakım yapmadan önce GDPR'nin 35. maddesinin kilit noktalarından biri olan veri koruma etki değerlendirmesini gerçekleştirmek için kullanılabilir.
Konum raporları	Kuruluşunuzda veri giriş çıkışı oldukça bu verileri koruyabilmek ve şifreleyebilmek oldukça önemlidir. Ancak bu verilerin sahiplerinin durum ve coğrafi konumlarını tespit etmek ve raporlamak da gerekir. Bu sadece üretim verileriniz için değil bu verilerin tüm kopyaları için de geçerlidir. Veeam Availability Suite 9.5 Güncelleme 3 ile bütün veri noktalarının konumunu etiketleyebilecek ve tüm üretim verileri ve bu verilerle ilgili yedekler, yedek kopyaları, teypler ve replikalar, verilerin coğrafi konumları ve bu konumlar arasında uyuşmazlık olup olmadığı hakkında rapor hazırlayabileceksiniz. Bu özellik, GDPR'nin 15 ve 44. maddeleri ile bütünlüğü sağlamak için hayati önem taşır.
Uçtan uca şifreleme	GDPR'nin 44. maddesi AB sınırları içerisinde ve dışarısındaki bölgeler veya uluslararası coğrafyalar arasındaki veri aktarımlarıyla ilgilidir. Bu süreçler boyunca veri sahipleri ile ilgili bilgileri güvenli şifreleme kullanarak iletmek son derece önemlidir. Veeam yerleşik olarak uçtan uca AES 256-bit şifreleme sağlayarak sizlere yedek dosyaları ve verileri kaynağında (yedekleme esnasında), hareket halindeyken ve hareketsizken şifreleme olanağı sunar. Bu özellik, kuruluşunuzun ve kuruluşunuza bağlı şirketler veya birliklerin tamamının GDPR'nin 32 ve 44. maddeleriyle uyumluluk sağlaması için çok önemlidir.
Rol tabanlı erişim kontrolleri	GDPR maddelerinin birçoğu etkinliklerin rapor edilmesi, günlüklerinin tutulması ve kimin hangi verilere erişebileceğinin tanımlanmasıyla ilgili. Veeam Availability Suite'te ortamınızdaki bazı veri noktalarına erişimi kısıtlamanıza olanak sağlamak üzere yerleşik RBAC kontrolleri bulunuyor. Veeam Availability Suite'in bir parçası olan Veeam Backup Enterprise Manager ile son kullanıcılarınıza self servis imkanı sunabilir, ihtiyaç duyulduğunda bazı verilere erişimi kısıtlayabilir veya erişim hakkı verebilirsiniz.
Veri dışlama	Bazı veriler özellikle işlenmelidir (hatta bazıları dışlanmalıdır - GDPR 9. madde) ve bu işlemenin raporları tutulmalıdır (GDPR 30. madde). Veeam Availability Suite'te dışlamaları kullanarak ajanlarla sanal makine, disk ve hatta dosya/klasör bazlı verileri kolayca dışlayabilir, böylece uyumlu kalabilirsiniz.