VEEAM

DSGVO: Fünf Lektionen basierend auf der Compliance-Erfahrung von Veeam

Zusammenfassung für Führungskräfte

Mark Wong
General Counsel

Einführung

In diesem Whitepaper beschreiben wir unsere Sichtweise auf die Bedeutung der DSGVO für unser Unternehmen. Informationen zur DSGVO finden Sie überall im Internet. Zahlreiche Firmen und Rechtsanwälte erklären sich zu Experten, dabei ist DSGVO-Compliance jedoch eine individuelle Aufgabe für Unternehmen. Sie kennen Ihr Unternehmen von Grund auf. Somit sind Sie in der besten Position, um ein wahrer Experte zur DSGVO-Compliance in Ihrem Hause zu werden. Wir möchten die im Rahmen unseres eigenen Compliance-Verfahrens gesammelten Erfahrungen und gelernten Lektionen mit Ihnen teilen. So können Sie Ihren Weg zur DSGVO-Compliance besser verstehen und zudem Softwarelösungen von Veeam kennenlernen, die eine wichtige Rolle für Ihre Datenmanagement- und Datenschutzstrategie spielen und dafür sorgen können, dass Ihr Unternehmen Always-on ist.™.

Dieses Whitepaper ist eher technisch orientiert: Wir werden unsere Ansichten zur DSGVO aus einer technischen und rechtlichen Compliance-Perspektive erörtern. Wir werden die Grundlagen der DSGVO beleuchten und untersuchen, wie die DSGVO zu einem Gesetz wurde, das in Europa neue Maßstäbe im Datenschutz setzt und die Datenschutzrichtlinie von 1995 ersetzt. Die entscheidenste Neuerung besteht darin, dass die DSGVO die Kontrolle über personenbezogene Daten wieder an die betroffene Person zurückgibt, während Unternehmen, die personenbezogene Daten sammeln, verarbeiten, analysieren und verwenden, gegenüber der Person nun zusätzliche Pflichten haben. Datenschutz ist ein Grundrecht von Menschen, und jedes Unternehmen, das personenbezogene Daten verarbeitet, muss dafür sorgen, dass diese Daten rechtmäßig verwendet und mit den gleichen Standards geschützt werden, die auch für vertrauliche Informationen gelten. Wir glauben, dass unsere Produkte und Lösungen Ihrem Unternehmen dabei helfen können, die Verfügbarkeit zu maximieren und zu einem Always-On Enterprise zu werden.

Wann tritt die DSGVO in Kraft?

Am 25. Mai 2018. Die DSGVO wurde am 27. April 2016 veröffentlicht. Es wurde jedoch ein Übergangszeitraum von zwei Jahren eingeräumt, damit Unternehmen die Umstellung von der Datenschutzrichtlinie auf die strengeren Anforderungen der DSGVO bewältigen können.

Was verlangt die DSGVO von Unternehmen?

Die DSGVO basiert auf fünf (5) Grundsätzen.

1. **Machen Sie sich mit Ihren Daten vertraut.** Ermitteln Sie alle personenbezogenen Daten, die Ihr Unternehmen sammelt, und finden Sie heraus, wer Zugriff darauf hat.
2. **Verwalten Sie die Daten.** Legen Sie Regeln und Prozesse für das Aufrufen und Verwenden personenbezogener Daten fest.
3. **Schützen Sie die Daten.** Implementieren Sie Sicherheitsmaßnahmen und gewährleisten Sie, dass diese Maßnahmen Daten zuverlässig schützen und eine Reaktion auf Sicherheitsverletzungen möglich machen.
4. **Dokumentieren und sorgen Sie für Compliance.** Dokumentieren Sie Ihre Prozesse, stellen Sie Datenanfragen und melden Sie jegliche Probleme oder Sicherheitsverletzungen, die von den Richtlinien abgedeckt werden.
5. **Kontinuierliche Optimierung.** Unsere digitale Welt verändert sich ständig. Veeam glaubt, dass sich die digitale Welt in den kommenden fünf Jahren noch schneller weiterentwickeln wird als in den zehn Jahren zuvor. Unternehmen müssen ihre vorhandenen Verfahren und Protokolle kontinuierlich evaluieren und testen sowie an neue Gegebenheiten anpassen.

Warum gibt es keine Standardlösung für DSGVO-Compliance?

Das Gesetz ist zwar für alle gleich. Unternehmen, die das Gesetz einhalten müssen, sind jedoch unterschiedlich und sammeln, verwalten, nutzen und schützen Daten auf verschiedene Weise. Außerdem variieren die personenbezogenen Daten, da es sich dabei um eine breit angelegte Informationskategorie handelt. Im Allgemeinen werden sie als jegliche Daten definiert, die sich zur Identifizierung einer Person verwenden lassen. Dazu gehören Online-IDs (IP-Adressen), Name, Kontaktdaten, Vertriebsdatenbanken, Daten aus dem Kundensupport, Formulare mit Kundenfeedback, Standortdaten, Videoaufzeichnungen, Prämienprogramme, Gesundheits- und Finanzdaten usw. Zudem gibt es eine Kategorie für sensible personenbezogene Daten, die Rasse, ethnische Abstammung, Gesundheit und sexuelle Orientierung umfassen kann. Die Richtlinien für Verarbeiter solcher sensiblen personenbezogenen Daten sind noch strenger als bei „normalen" oder „regulären" personenbezogenen Daten. Zwar sehen sich viele Unternehmen in einer ähnlichen Situation, doch gibt es zahlreiche Unterschiede hinsichtlich Volumen, Art, Aufgabe und vor allem Personen. Eine der entscheidenden Komponenten für DSGVO-Compliance besteht in der Schulung des Personals zum Umgang mit personenbezogenen Daten.

Welche Änderungen werden im Rahmen der neuen DSGVO erwartet?

Die DSGVO wurde verabschiedet, um ein breites Spektrum an Anforderungen zu definieren, die Unternehmen bei der Sammlung oder Verarbeitung personenbezogener Daten beachten müssen. Aufgabe und Grundsätze der DSGVO sind:

1. **Fairness und Transparenz für einzelne Personen.** Unternehmen müssen Personen darüber informieren, dass ihre personenbezogenen Daten für einen rechtmäßigen Zweck verwendet werden.
2. **Einschränkung der Nutzung auf das, was erforderlich ist.** Unternehmen dürfen personenbezogene Daten ausschließlich für explizite, spezifische und legitime Zwecke verwenden. Personenbezogene Daten dürfen ausschließlich für den Zweck genutzt werden, über den die jeweilige Person informiert wurde.
3. **Sammeln Sie nur, was Sie brauchen.** Es gibt ein breites Spektrum an personenbezogenen Daten; Unternehmen dürfen jedoch nur solche personenbezogenen Daten sammeln, die sie benötigen und die dem Zweck angemessen sind.
4. **Akkuratesse und Recht auf Vergessenwerden.** Unternehmen sind nun dazu verpflichtet, akkurate Datensätze zu pflegen, und müssen Anfragen von Personen zur Korrektur ihrer personenbezogenen Daten erfüllen. Außerdem müssen Unternehmen den Wunsch von Personen auf Vergessenwerden respektieren, was bedeutet, dass Unternehmen entsprechende personenbezogene Daten so weit wie möglich löschen müssen.
5. **Begrenzte Speicherung.** Personenbezogene Daten dürfen lediglich so lange gespeichert werden, wie es zum Erfüllen des ausdrücklichen legitimen Zwecks erforderlich ist.
6. **Schutz der Daten.** Unternehmen müssen Schritte ergreifen, um personenbezogene Daten durch organisatorische und technische Maßnahmen (wie Software oder Verschlüsselung) zu schützen.
7. **Ernennung eines Datenschutzbeauftragten.** Diese Position wird als Anforderung für die umfassende Überwachung von Daten eingeführt und beinhaltet Expertenwissen über Datenschutzgesetze und -praktiken. Der Datenschutzbeauftragte untersteht direkt der höchsten Managementebene.

Wer muss die DSGVO einhalten?

Unternehmen in der Europäischen Union (EU), die personenbezogene Daten verarbeiten, bzw. sämtliche Unternehmen außerhalb der EU, die personenbezogene Daten von EU-Bürgern verarbeiten, um Waren oder Dienstleistungen anzubieten bzw. das Verhalten von EU-Bürgern zu überwachen (z. B. soziale Medien). Eine wichtige Änderung im Vergleich zur Datenschutzrichtlinie von 1995 besteht darin, dass die Datenschutzrichtlinie ausschließlich für „Datenverantwortliche" bzw. solche Personen galt, die Daten selbst sammeln und verarbeiten. Die DSGVO hingegen gilt auch für „Datenverarbeiter", also für Unternehmen, die personenbezogene Daten im Namen anderer verarbeiten.

Wie hoch sind die Strafen?

Einer der Hauptunterschiede zwischen der DSGVO und der alten Datenschutzrichtlinie besteht in den hohen Strafen, die im Rahmen der DSGVO verhängt werden können. So beträgt die Höchststrafe 4 % des Jahresumsatzes eines Unternehmens bzw. 20 Millionen Euro (je nachdem, was höher ist). Beachten Sie, dass es sich dabei um eine Maximalstrafe handelt, die je nach Sicherheitsverletzung variieren kann.

Was ist eine rechtliche Grundlage zur Verarbeitung personenbezogener Daten?

Gemäß der DSGVO gibt es verschiedene Grundlagen, inklusive der zu einer Verarbeitung, die zur Ausführung eines Vertrags erforderlich ist. Die Person stimmt der Verarbeitung der personenbezogenen Daten zu, oder ein Unternehmen hat ein reales, legitimes Interesse an diesen Daten, was das Recht einer Person auf Datenschutz überwiegt.

Worin besteht der Unterschied zwischen organisatorischen und technischen Sicherheitsmethoden?

In der DSGVO werden sowohl organisatorische als auch technische Methoden zum Schutz personenbezogener Daten beschrieben. Organisatorische Sicherheitsmethoden laut DSGVO können die Begrenzung der Zahl von Personen in Ihrem Unternehmen beinhalten, die Zugriff auf personenbezogene Daten haben, während eine technische Methode zum Beispiel darin bestehen kann, dass für den Zugriff auf personenbezogene Daten bestimmte Passwörter oder Verschlüsselungen erforderlich sind. Die DSGVO überlässt es Unternehmen zu entscheiden, welche Sicherheitsmaßnahmen bzw. Kombinationen aus Sicherheitsmaßnahmen ausreichen, um die jeweiligen personenbezogenen Daten zu schützen.

Welche Art von Datenaufbewahrung verlangt die DSGVO?

Zum Schutz personenbezogener Daten setzt die DSGVO auf Audits, Verfahren und verbesserte Prozesse. Unternehmen müssen Aufzeichnungen über ihre Datenverarbeitungsaktivitäten und ganz besonders über die Übertragung personenbezogener Daten an Orte außerhalb der EU aufbewahren. Eine Dokumentation der ergriffenen Sicherheitsmaßnahmen ist Pflicht. Unternehmen sind dafür verantwortlich, die entsprechenden Bewertungen vorzunehmen. Es gibt jedoch zahlreiche Dienstleister, die einschlägige Beratung anbieten.

Dürfen personenbezogene Daten an Orte außerhalb der EU übertragen werden?

Ja, die DSGVO ist jedoch sehr strikt, was die Übertragung personenbezogener Daten von EU-Bürgern an Orte außerhalb der EU betrifft. Es gibt bestimmte Mechanismen wie Verträge oder Zertifizierungen, die eine solche Übertragung ermöglichen.

Wie sieht es mit Lieferanten und Partnern aus, die möglicherweise Zugriff auf personenbezogene Daten haben, welche unser Unternehmen gesammelt hat?

Verarbeiter müssen gemäss DSGVO den Datenverantwortlichen garantieren, dass geeignete technische und organisatorische Sicherheitsmaßnahmen für den Erhalt und die Verarbeitung personenbezogener Daten implementiert wurden. Wenn sich Ihr Unternehmen auf Lieferanten und Drittanbieter verlässt, um personenbezogene Daten zu verarbeiten, die Ihr Unternehmen gesammelt hat, müssen Sie sicherstellen, dass diese Anbieter ebenfalls DSGVO-konform sind und Ihnen eine entsprechende Garantie geben.

Kurzinfo zur DSGVO:

- Die DSGVO verschafft einzelnen Personen die Kontrolle über ihre personenbezogenen Daten. Unternehmen müssen Personen darüber informieren, warum sie personenbezogene Daten verarbeiten.
- Personen haben das Recht, eigene personenbezogene Daten korrigieren oder löschen zu lassen bzw. zu verlangen, dass diese nicht weiter verarbeitet werden (Opt-Out).
- Personen haben das Recht auf Datenübertragbarkeit, das bedeutet, dass Unternehmen Personen auf Wunsch diesbezüglich unterstützen müssen.
- DSGVO-Compliance endet nicht am 25. Mai 2018. Vielmehr handelt es sich um einen Prozess der kontinuierlichen Verwaltung, Überwachung und Optimierung.

Wenn Sie mehr über den Weg von Veeam zur DSGVO-Compliance sowie die fünf Grundsätze erfahren möchten, laden Sie den Schritt-für-Schritt-Leitfaden für IT-Experten herunter: https://www.veeam.com/wp-gdpr-compliance-experience.html

Veeam® möchte seine Erfahrungen hinsichtlich der Einhaltung der Datenschutz-Grundverordnung (DSGVO) mit Ihnen teilen. Diese Verordnung ist komplex und faktenspezifisch, was bedeutet, dass sich DSGVO-Compliance-Programme von Unternehmen zu Unternehmen unterscheiden. Die DSGVO ist eine wichtige Aktualisierung der Datenschutzrichtlinie aus dem Jahr 1995 (Richtlinie 95/46/EG). Schließlich hat sich die Welt, in der wir leben, seit damals stark verändert.

Viele Unternehmen gehen davon aus, dass die DSGVO lediglich ein Thema für die IT ist. Das ist jedoch nicht richtig. Die Verordnung betrifft alle – und keineswegs nur die IT.

Wir haben dieses Whitepaper erarbeitet, um zu beschreiben, wie Veeam die DSGVO zum Zeitpunkt der Veröffentlichung interpretiert. Als privates IT-Unternehmen, das Backup-, Disaster-Recovery- und Datenmanagement-Software für virtuelle, physische und cloudbasierte Workloads entwickelt, um Availability for the Always-On Enterprise™ sicherzustellen und für maximale Verfügbarkeit zu sorgen, haben wir viel Zeit auf die DSGVO verwendet – nicht nur, um als globales Unternehmen konform zu werden, sondern auch um unsere Produkte weiterzuentwickeln.

Dieses Whitepaper dient nicht zur rechtlichen Beratung bzw. Ermittlung dessen, was die DSGVO für Ihr Unternehmen bedeutet. Wir empfehlen Ihnen (so wie wir es gehandhabt haben), die DSGVO mit Rechtsexperten zu besprechen und zu erörtern, welche Gültigkeit sie für Ihr Unternehmen hat. Gemeinsam mit den Spezialisten sollten Sie dann einen Plan zur Gewährleistung der Compliance erarbeiten. Veeam stellt dieses Whitepaper im Ist-Zustand bereit und übernimmt keinerlei explizite oder implizite Garantie hinsichtlich der Informationen in diesem Whitepaper.

Veröffentlicht im Januar 2018. Version 1.0

Über Veeam Software

Veeam® kennt die neuartigen Herausforderungen, die Unternehmen weltweit bewältigen müssen, um für ein Always-On Business™ zu sorgen, das rund um die Uhr verfügbar. Darum hat Veeam einen neuen Verfügbarkeitsmarkt für Always-On Enterprise™ entwickelt und unterstützt Unternehmen dabei, bei allen Anwendungen und Daten RTOs und RPOs (RTPO™) von unter 15 Minuten einzuhalten. Eine von Grund auf erneuerte Lösung sorgt dabei für eine schnellere Datenwiederherstellung, Verhinderung von Datenverlusten, verifizierten Schutz, nutzbare Daten und umfassende Transparenz. Die Veeam Availability Suite™, die Veeam Backup & Replication™ umfasst, greift auf Virtualisierungs-, Speicher- und Cloud-Technologien für moderne Rechenzentren zurück, damit Unternehmen Zeit sparen, Risiken mindern und Kapital- sowie Betriebskosten spürbar senken können.

Veeam wurde 2006 gegründet und hat inzwischen 51.000 ProPartner sowie mehr als 282.000 Kunden weltweit. Die globale Hauptniederlassung des Unternehmens befindet sich in Baar (Schweiz). Außerdem hat Veeam weitere Niederlassungen auf der ganzen Welt. Wenn Sie mehr erfahren möchten, besuchen Sie https://www.veeam.com/de.

VEEAM IST STOLZ AUF SEINE

1 MILLION
BENUTZER

51.000
PARTNER

282.000
KUNDEN

80
FÜHRENDE BRANCHENAUSZEICHNUNGEN

GLOBAL ALLIANCE-PARTNER

BLEIBEN SIE AUF DEM LAUFENDEN

Veeam Software
@veeam_software
@Veeam_Nordics
Veeam Software
Veeam
www.veeam.com