VEEAM

GDPR: 5 Lessons Learned Veeam Compliance Experience Shared

CIO Summary

Mark Wong
General Counsel

Introduction

The purpose of this white paper is to offer you the Veeam perspective of what the GDPR means to us. GDPR information is broadly available across the internet, and while many companies and lawyers may position themselves as experts, GDPR compliance is unique to each organization. You know your organization best, so you are in the best position to become the true expert in GDPR compliance for your organization. We will share our insights and lessons that we learned through our own compliance to help you on the path to thinking about not only GDPR compliance, but how Veeam's software solutions can play a critical role in your data management and protection strategies and ensure that your organization is Always-On™.

This white paper is intended to be more technical and we will discuss and explain our view of GDPR from a technical and legal compliance perspective. We will examine the principles behind GDPR and how GDPR evolved to first benchmark law governing data privacy in Europe since the Data Protection Directive it replaces that was originally enacted in 1995. The most notable change is that GDPR puts the control over personal data back into the hands of the individual and organizations that collect, handle, analyze and use personal data have more obligations to the individual. Data privacy is an individual's fundamental right and any organization that handles personal data should be focused on using the data in a lawful manner and protecting it with same standards it protects its confidential information. We believe our products and solutions can help your organization ensure Availability for your Always-On Enterprise.

When is GDPR effective?

May 25, 2018. GDPR became law on April 27, 2016, but included a two-year transition period allowing organizations to make the transition from the Data Protection Directive to the broader requirements of GDPR.

What does GDPR really ask organizations to do?

GDPR is broken down into five (5) basic principles.

1. **Know your data.** Identify the personally identifiable information (PII) your organization collects and who has access to it.
2. **Manage the data.** Establish the rules and processes to access and use PII.
3. **Protect the data.** Implement and ensure security controls are in place to protect the information and respond to data breaches.
4. **Document and comply.** Document your processes, execute data requests and report any issues or data breaches within the guidelines.
5. **Continuous improvement.** Our digital world is constantly evolving and Veeam believes our digital world will change more in the next five years than it has in the last 10 years. Organizations must constantly evaluate and test their existing procedures and protocols and evolve and enhance them as our digital world advances.

Why isn't there a one-size-fits-all solution to GDPR compliance?

While the law is the same, the organizations that must comply with the laws are unique and the ways organizations collect, manage, use and protect data is different. The PII is also different as it is a broad category of information, and is generally defined as any data that can be used to identify an individual. This includes online identifiers (IP address), name, contact information, sales databases, customer support data, customer feedback forms, location data, video footage, rewards programs, health and financial information, and more. There is also a category of sensitive PII, which can include race, ethnic origin, health and sexual orientation. The guidelines for processors of this type of sensitive PII is even stricter than "regular" or "ordinary" PII. While many organizations will face similar situations, the variation comes in volume, type, purpose and most importantly, people. One of the critical components of GDPR compliance is training people to handle PII.

What are the changes expected under the new GDPR regulation?

GDPR was enacted to implement a broad range of requirements on organizations that collect or process PII. The mission and principles of GDPR are:

1. **Providing fairness and transparency to individuals.** Organizations must inform individuals how their PII is being used for a lawful purpose.
2. **Limiting the use to what's necessary.** Organizations can only use the PII for an express, specified and legitimate purpose. The PII can only be used for the reason or purpose that was disclosed to the individual.
3. **Collect only what you need.** There is a broad range of PII and an organization should only collect the PII it needs and is adequate for the purpose.
4. **Accuracy and the right to be forgotten.** Organizations now have a duty to maintain accurate records and must execute on requests from an individual to correct their PII. Organizations must also respect an individual's desire to be forgotten, meaning the organization must erase the PII to the extent possible.
5. **Limited storage.** The PII should only be stored for the period of time necessary to complete the express legitimate purpose.
6. **Secure the data.** Organizations have to take steps to secure PII through process and technical measures such as software or encryption.
7. **Appointment of a data protection officer.** This position will be introduced as a requirement for large scale monitoring of data and will involve expert knowledge of data protection laws and practices, and he/she will be required to directly report to the highest level of management.

Who has to comply with GDPR?

Organizations in the EU that process PII or any organization outside of the EU that processes PI of EU residents for the purpose of offering services, goods or monitoring their behavior (e.g., social media). A major shift from the Data Protection Directive is that the Data Protection Directive only applied to "controllers," or those who collected and processed data themselves. GDPR also applies to "processors," meaning companies that process PII on behalf of others.

What are the fines?

One of the major differences between GDPR and the Data Protection Directive is that significant fines can be levied under the GDPR, where the maximum fine is the greater of 4% of your organization's global revenue, or 20 million euros. Note that this is a maximum fine and it will vary depending on the breach.

What's a legal basis for processing PII?

There are several grounds provided by GDPR, including the processing when necessary to perform a contract. The individual consents to the processing of the PII or if an organization has a bona fide legitimate interest that outweighs an individual's right to privacy.

What is the difference between organizational method and technical method to security?

GDPR discusses both organizational and technical methods to keep PII secure. Organizational methods of security under the GDPR can mean limiting the number of people in your organization who have access to the PII and a technical method can be requiring specific passwords to access the PII or encryption. GDPR leaves the judgement to the organization to determine which or what combination of security measures are sufficient to protect the PII that is involved.

What type of record keeping does GDPR require?

GDPR requires audits, procedures and enhanced processes to protect PII. Organizations are required to keep records of their data processing activities and especially transfers of PII outside the EU. Documentation of the security measures taken place is a must. Organizations are responsible for carrying out assessments themselves, although there are many vendors who provide guidance and advice.

Can I transfer PII outside of EU?

Yes, but the GDPR is very strict about the transfer of PII of European residents outside of the EU. There are certain mechanisms, such as a contract or certification that enables these transfers.

What about my vendors and partners that may have access to the PII that my organization has collected?

GDPR processors to guarantee to controllers that the appropriate technical and organizational security measures are in place to receive and process the PII. If your organization uses vendors and third parties to use PII that your organization has collected, make sure they are also GDPR compliant and will guarantee you that they are.

Quick points about GDPR:

- GDPR gives the individual the power to control their PII. Organizations have to let individuals know why they are processing the PII.
- Individuals have the right to have their PII corrected or deleted and ask that it no longer be processed (opt out).
- Individuals have a right to data portability, so organizations have to provide assistance to the individual if they request it.
- GDPR compliance doesn't end on May 25, 2018. It is a constant and ongoing process of continuous management, monitoring and improvement.

To learn more about Veeam's road to GDPR compliancy and the five key principles, download the step-by-step guide for IT professionals: https://www.veeam.com/wp-gdpr-compliance-experience.html

Veeam® is committed to sharing our General Data Protection Regulation (GDPR) compliance experience with you. This regulation is complex and fact specific, meaning each organization's GDPR compliance program may mean something different from the next company. GDPR is a major update to the Data Protection Directive from 1995 — more specifically 95/46/EC — and the data intensive world we live in is significantly different than the world we lived in 1995.

Many people might think that the GDPR is just an IT issue, but that is the furthest from the truth. It affects everyone — not just IT.

We have prepared this white paper as a discussion of how Veeam interprets GDPR as of the date of publication. As a privately held information technology company that develops backup, disaster recovery and data management software for virtual, physical and cloud-based workloads to provide Availability for the Always-On EnterpriseTM, we have spent a lot of time with GDPR not only complying with it as a global organization, but also in development of our products.

This white paper should not be relied upon as legal advice or determination on how GDPR applies to your organization. We encourage you to do as we did, and work with legally qualified professionals to discuss GDPR and how it applies to your organization and collaborate and build a plan towards compliance. Veeam provides this white paper "as is" and makes no express or implied warranties as to the information in this white paper.

Published on January 2018. Version 1.0

About Veeam Software

Veeam® recognizes the new challenges companies across the globe face in enabling the Always-On Business™, a business that must operate 24.7.365. To address this, Veeam has pioneered a new market of Availability for the Always-On Enterprise™ by helping organizations meet recovery time and point objectives (RTPO™) of < 15 minutes for all applications and data, through a fundamentally new kind of solution that delivers high-speed recovery, data loss avoidance, verified protection, leveraged data and complete visibility. Veeam Availability Suite™, which includes Veeam Backup & Replication™, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs.

Founded in 2006, Veeam currently has 51,000 ProPartners and more than 282,000 customers worldwide. Veeam's global headquarters are located in Baar, Switzerland, and the company has offices throughout the world. To learn more, visit http://www.veeam.com.

VEEAM IS VERY PROUD OF OUR

1M
USERS

51K
PARTNERS

282K
CUSTOMERS

80
TOP INDUSTRY AWARDS

GLOBAL ALLIANCE PARTNERS

Cisco Preferred Solution Partner
DELL EMC
Hewlett Packard Enterprise
Gold Microsoft Partner
NetApp ALLIANCE PARTNER
vmware PARTNER TECHNOLOGY ALLIANCE

STAY CONNECTED

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