GDPR: 5 Lessons learned

Veeam compliance experience shared

25 May 2018
THE GDPR WILL COME INTO FORCE
BE COMPLIANCE READY

The General Data Protection Regulation (GDPR) requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. You must be able to guarantee the safety of all the personal data you collect and/or process — or potentially face penalties.

Discover the five key lessons learned by Veeam® on our way to GDPR compliance, and accelerate your GDPR efforts. It's not too late!

GDPR compliance cannot be achieved by using a single solution

GDPR encompasses all layers of the company including employee awareness, business and governance processes, monitoring and reporting, and information systems.

Non-compliance penalties of 4% of Annual Global Turnover or 20 Million Euro

Affect of companies processing personal data of people in EU

Data Protection Offices (DPO) may be required

Notify authorities and individuals of a breach within strict timelines

Consent must stand out, be clear and include the reasons for collection

People can decide to revoke access to their data

People have the right to obtain, change, move and delete their data

Include data protection at the design stage for a new system

What does GDPR really ask organizations to do? Five fundamental lessons learned by Veeam:

1. **Know your data** — Identify the personally identifiable information (PII) your organization collects, has and who has access.
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 on data requests and report any issues or data breaches within the guidelines.
5. **Constantly review and improve** your processes and procedures for data privacy and protection.

Veeam Availability Suite provides deep insight into data protection, auditing and reporting with enterprise class features to assist your journey to become GDPR compliant.

EU GDPR articles on data management and the Veeam framework	Article 5 — Principles relating to processing of personal data Article 6 — Lawfulness of processing Article 9 — Processing of special categories of personal data Article 15 — Right of access by the data subject Article 17 — Right to erasure (right to be forgotten) Article 20 — Right to data portability Article 25 — Data protection by design and by default Article 30 — Records of processing activities Article 32 — Security of processing Article 35 — Data protection impact assessment Article 39 — Tasks of the data protection officer Article 44 — General principle for transfers
Availability of your data	GDPR article 32 explains that you need to make the data available again in case of a disaster, malware (ransomware) attack or other issues. With Instant VM Recovery®, you can quickly make your data available again and Veeam Backup & Replication™ has 50+ recovery possibilities on a single backup. GDPR article 20 requires you to return data that you own on a subject to him or her. Veeam's advanced recovery capabilities give you the possibility to explore backups and replicas and recover the data into common formats so you can deliver that data to the subjects in a timely manner.
Tagging of PII data and analytics	When PII data is identified, it is critical to monitor and audit with constant diligence. With Veeam ONE™, you can tag your infrastructure sources if they contain PII and run reports on them, review dashboards and do audits on certain activities (e.g., what is restored and who performed the restores) in your environment. These are important parts of GDPR articles 6, 32 and 35 as well as for the data protection officer to perform his duties from GDPR article 39.
Data retention and the right to be forgotten	While the right to be forgotten (GDPR article 17) is not absolute, you cannot keep data for longer than it is legally necessary (depending on country laws and vertical segments). With data retention, you can clearly mark backups obsolete and Veeam Backup & Replication will remove the data retention points when the retention has passed which is described in GDPR article 6.
Data discovery	One of the first tasks an organization needs to do in its journey to GDPR compliancy is to discover what data is owned. Investigation of data sources is not always easy in production. Veeam Availability Suite™ with Veeam Explorer™ technology, guest file indexing and Virtual Labs give your organization the ability to perform discoveries of the data that reside in your copies.
SureBackup, SureReplica and Virtual Labs	SureBackup and SureReplica are intended to automate and simplify the backup verification process. This is the most crucial part of data management and protection when adhering to the protection of private subject data in GDPR articles 5 and 25. You can automatically verify every created restore point of every VM or replica and ensure that they will function as expected in the event you are required to redeem or report on these invaluable restore points. This provides your data processor team the necessary tools to comply with the various elements of the GDPR framework in a seamless method. Virtual Labs, which is the underlying technology, can be used to perform data protection impact assessments before you perform updates, upgrades or maintenance to your production data which is a key item of GDPR article 35.
Location reports	As data moves in and out of your organization, it is crucial to be able to protect and encrypt. However, it is also necessary to pinpoint and report on the geographical location and state of these data subject records. This applies to your production data but also to all copies of that data. With Veeam Availability Suite 9.5 Update 3, you will be able to tag the location of each data point and report on all production data and the relevant backup, backup copies, tapes and replicas, their geographical location and whether there is a mismatch between locations. This is vital in maintaining integrity to GDPR article 15 and article 44.
End-to-end encryption	GDPR article 44 refers to data transfer between regions or international geographies in and out of the European Union. During these processes, it is crucial to transmit data subject information using secure encryption channels. Veeam delivers built-in end-to-end AES 256-bit encryption, giving you the ability to encrypt backup files and data at source (during backup), in flight and at rest. This is paramount to comply with GDPR articles 32 and 44 throughout your organization and affiliate bodies or associations.
Role-based access controls	Many GDPR articles talk about logging of activities, reporting on those activities and defining who has access to what data. Veeam Availability Suite has RBAC controls built-in to allow you to restrict access to certain data points in your environment. With Veeam Backup Enterprise Manager, part of Veeam Availability Suite, you can also allow self-service to your end users, limit access to certain data or give access when it is needed for their responsibilities.
Excluding data	Some data should be processed specifically (or even excluded — GDPR article 9) and records should be maintained of that processing (GDPR article 30). By using exclusions in the Veeam Availability Suite, you can easily exclude data based on VMs, disks and even on file/folder basis with agents, keeping you in compliance.