EU General Data Protection Regulation (GDPR)

How Zerto Can Aid with Compliance

As of May 25th, 2018, the new EU General Data Protection Regulation (GDPR) is in effect. This legislation has been drafted to update the existing EU Data Protection directive which was crafted back in 1995.

Who does it apply to?

GDPR is designed to protect the rights and freedoms of citizens within the EU with regards to how personal data is collected, stored, used, and retained by others. It aims to introduce a common standard of information security across the EU and furthermore, ensure that standard of protection applies to any organization, regardless of location, that processes the personal data of any EU citizen.

Why do I need to comply?

GDPR features far more stringent data protection regulations than ever before. Significantly larger fines have been implemented to enforce these regulations for organizations that breach GDPR. These fines can range up to €20,000,000 (approx. $25,000,000), or 4% of the parent company's global annual revenue – whichever is greater.

Article 32 – Security of Processing

Article 32 of GDPR enacts the legal requirement for organizations to ensure that data and infrastructure is resilient and protected. Any company that GDPR affects must be protected from internal and external threats, including technical failures, human errors, and malicious malware attacks. The article also specifies organizations must be able to regularly demonstrate and prove the effectiveness of the measures used for security and protection.

What are some of the other major requirements of GDPR?	
Demonstrable Proof of Compliance (Articles 24, 28, 30, and 32)	Organizations must be able to regularly test the effectiveness of security measures and provide documented proof of compliance.
Data Protection by Design & by Default (Article 25)	Organizations must take a pro-active approach to security and ensure that protective measures are baked into the design of processing systems and services, rather than being added reactively.
The "State-of-the-Art" (Articles 25 and 32)	Organizations must give due consideration to the "State of the Art" when implementing measures designed to ensure the protection and security of systems and services.
Transfer of personal data to third countries or international organisations (Chapter V)	Organizations must consider the location of where the personal data resides and may have to take additional steps before it can move data to services and/or resources that are located in a third country.

What is Zerto Virtual Replication (ZVR)?

ZVR is a state-of-the-art IT Resilience platform that enables organizations to ensure the protection, availability, and resilience of all systems and services. Zerto not only ensures availability with RPOs of seconds and RTOs of minutes, but helps organizations to build a stable, unified, and flexible infrastructure that provides ongoing resilience against modern threats.

Zerto helps organizations ensure compliance with a wide variety of regulations at industry, regional, and international levels, including GDPR.

Article 32 – Security of Processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the **pseudonymisation and encryption** of personal data;	Zerto's technology agnostic approach means transparency to any type of network, storage or guest-based encryption method, giving you the freedom to choose the solutions that best meet your requirements.
(b) the ability to ensure the ongoing confidentiality, **integrity, availability and resilience** of processing systems and services;	Zerto provides Continuous Data Protection (CDP) that ensures the write-order fidelity of multi-VM applications with near-zero data loss— guaranteeing the integrity of replicated data. Seamless data mobility and infrastructure flexibility, across both on-premises and cloud environments, enables organizations to not only maximize the availability of, but also ensure the ongoing resilience of processing systems and services in the face of increasing threats and constant change.
(c) the ability to **restore the availability and access to personal data in a timely manner** in the event of a physical or technical incident;	Zerto provides Recovery Point Objectives (RPOs) of seconds and Recovery Time Objectives (RTOs) of minutes, with fully automated and orchestrated recovery of even complex, multi-VM application stacks. Rewind and recover from any physical or technical incident – even ransomware – with just 4 simple steps, choosing from potentially thousands of recovery points in increments of seconds for up to 30 days in the past. Zerto's Long-Term Retention capabilities extend these capabilities with the ability to archive point-in-time captures for up to 1 year.
(d) a process for **regularly testing, assessing and evaluating the effectiveness** of technical and organisational measures for ensuring the security of the processing.	Zerto's IT Resilience platform provides fully automated, non-disruptive, and granular failover testing in isolated bubble networks for recovery assurance, with detailed reporting functionality to document proof of compliance during audits and inspections. A single person can test recovery operations in minutes with just 4 simple steps, without impacting protection and without impacting or disrupting production workloads. Zerto offers a consistent user experience across any type of technology by providing an easy to use management GUI, Mobile App and web-based analytics portal with SLA driven dashboards that provide you with a quick overview of the health of your environment and allows you use long term reporting for SLA reporting, protection environment sizing and/or trend analysis. The ability to test the recovery process combined with reporting (both on recovery and SLA) is very important as it is required to prove compliance (also see articles: 24 and 28).

Chapter V - Transfer of Personal Data to Third Countries or International Organisations

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Articles 44 – 50;
Chapter V of the GDPR sets out rules relating to international transfers of personal data. The European Commission can find that a third country provides an adequate level of protection for personal data, allowing personal data to be transferred there legally. If a country that you want to transfer personal data to is not "adequate", extra steps have to be taken before the transfer can take place.

Besides protecting your data, Zerto also offers great mobility capabilities allowing you to migrate applications and data in minutes across any distance. This allows you to act in a timely and controlled fashion when data residency rules change. Zerto's extensive global Cloud Service Provider eco-system, consisting of more than 350 providers, also allows you to select a Multi-Cloud or hybrid cloud strategy that best fits your needs regarding compliance and data residency.

About Zerto

Businesses need to be available to their customers, 24/7/365. Zerto provides Resilience for Evolving IT™ by ensuring enterprises and their customers always have access to business-critical applications without any IT interruption, downtime or delay. Zerto's award-winning Cloud Continuity Platform is the simplest, most reliable BC/DR software solution built to protect applications on any virtualized IT environment — be it public, private or hybrid cloud. Zerto's proactive approach to recovery gives companies the confidence they need to withstand any disaster, easily incorporate new technology, and quickly adapt to accommodate evolving IT and business priorities. **www.zerto.com**

09779