Zerto – Compliance with the EU GDPR

Background on the GDPR

Introduction. In May 2018, new European General Data Protection Regulation (the "GDPR") entered into effect.

It spans dozens of pages and imposes burdensome obligations on companies and organizations in virtually every aspect of collecting, processing, handling and storing personal data. At the same time, the GDPR enhances the rights given to data subjects to control personal data collected about them and to seek remedies.

Zerto has developed this document to explain about representative examples of GDPR requirements and how Zerto aims to comply with them.

Applicability. The GDPR applies to businesses established in the EU. It can also apply to business established outside the EU who offer their product and services to their EU business customers. Those EU business customers are subject to the GDPR and are required to flow-down their GDPR obligations onto their non-EU providers.

Because Zerto operates business in the EU, and because Zerto offers products and services to EU business customers, we have determined that the GDPR applies to Zerto.

Zerto's operations are up to par with the GDPR, with Zerto following technological, organizational, procedural and legal steps to ensure its ongoing compliance.

Data Stream Mapping

Zerto has canvassed the various personal data streams and data sources flowing through the company and has identified and documented the use cases for the data. This serves both as a basis for GDPR preparedness and as a basis for compliance with the GDPR's requirement of maintaining documented records of data processing activities.

Transparency

Under the GDPR's principle of 'transparency', organizations are required to take appropriate measures to provide information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form. The GDPR encourages the provision of such information in writing, including, where appropriate, by electronic means.

Zerto's privacy policy serves as the main mechanism for compliance with the GDPR's transparency obligations, to describe Zerto's practices with respect to personal data and to explain how Zerto facilitates data subjects' exercise of their rights under the GDPR.

Data security

The GDPR requires organizations handling personal data to implement appropriate technical and organizational measures to secure personal data, including encryption and security tests.

Zerto takes measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal data. These include encryption, data masking, audit logs, vulnerability scanning, physical security controls and backups.

Engaging subcontractors

The GDPR legitimizes the use of subcontractors for data processing activities, subject to several conditions.

For example, as required by the GDPR, Zerto performs due diligence into its subcontractors' data protection practices to confirm that the subcontractors provide sufficient guarantees that its processing will meet GDPR requirements. Zerto also has data processing agreements with these subcontractor that are consistent with GDPR requirements for such engagements.

Cross-border data transfers

The GDPR restricts the cross-border transfer of personal data to jurisdictions outside the European Economic Area (EEA). As a general rule, personal data may only be transferred to jurisdictions recognized by the EU Commission as having an adequate level of data protection, or otherwise transferred under appropriate safeguards.

Zerto and its subcontractors involved in personal data processing process personal data in member states of the European Economic Area, in territories or territorial sectors (e.g., Privacy Shield) recognized by an adequacy decision of the European Commission as providing an adequate level of protection for personal data or through recipients subject to adequate safeguards under the GDPR (e.g., Model Clauses).

This document is intended for informative purposes only. It does not constitute legal advice regarding the GDPR or any other matter, and may not be used or relied on for such purposes.