How Scality Can Help You with GDPR Requirements

A Scality White Paper

May 2018

SCALITY

How Scality Can Help You with GDPR Requirements

Introduction

After four years of preparation and debate, the GDPR (General Data Protection Regulation) was finally approved by the European Union Parliament on 14 April 2016. Enforcement date: 25 May 2018—at which time those organizations in non-compliance may face heavy fines.

The GDPR replaces the Data Protection Directive 95/46/EC. It was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. The key articles of the GDPR, as well as information on its business impact, can be found throughout this site (see: https://www.eugdpr. org/).

The GDPR not only applies to organizations located within the EU but also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of natural persons (referred to data subjects in GDPR) residing in the European Union, regardless of the company's location.

Based on GDPR regulations, the following key points should be considered in preparation for the GDPR compliance deadline. For situations where our storage technologies are concerned, the second section of this paper details how Scality can help customers meet the requirements of GDPR.

GDPR: Are You Prepared?

1. What major changes should companies expect with GDPR?

Only two decades ago, nearly all enterprise data was stored in corporate managed data centers and occasionally sent offsite to a physical archive such as Iron Mountain for longer-term retention. Corporate IT environments now include Remote Office/Branch Office (ROBO) as possible data repositories as well as public cloud services such as AWS S3, Microsoft Azure and other cloud file sharing services. Much of this enterprise data comprises information about customers, such as their contact and payment information in production systems such as databases, as well as backups and archives.

Prior to GDPR, it was the enterprise that decided where, when and how long to store this type of "personally identifiable Information" (PII) about people. This becomes a key concept subject to scrutiny under GDPR. For example, corporations must now prove the ability to identify all of their

Prior to GDPR, it was the enterprise that could decide about where, when and how long to store this type of "personally identifiable Information" (PII) about people. This becomes a key concept subject to scrutiny with GDPR."

data and show where it is stored and located. Moreover, there are now greater individual rights for people to decide how business will use their data, and even whether or not the data should be retained or forgotten.

There are therefore some major changes coming from GDPR that relate directly to data management:

- Data awareness and location: corporations must start with a complete picture about what data they are storing, where the data is located and on what systems or clouds it is stored. This has implications on inventory, search, reporting and auditing vast amounts of data and the storage systems holding that data.
- Sovereignty: GDPR also states that data must be stored and maintained within specific countries and locations of origin, and that data is not allowed to flow to external storage locations outside of those boundaries, or even to external clouds.
- Retention and "forget" requirements: business have started to preserve key data for a longer period of time, but GDPR forces new functions for purging/deleting some personally identifiable data, unless the business can prove it is required.

2. Who is expected to comply with GDPR?

GDPR has a decidedly global domain. It doesn't matter where the data is stored or where your company operates. If the "data subject" resides in the EU, the GDPR in general—and Article 17 in particular— apply. Secondly, "without undue delay" means days, not months. No excuse, justification, or defense is acceptable for non-compliance with an EU citizen's erasure request. Every instance and copy of their data in a company's possession must be expunged, and quickly. Never mind that right now, most companies could not track down every one of these instances — even if their corporate lives depended on it.

3. What can be expected should one not meet the new regulation?

Through GDPR, the European Union has now made data management rules uniform across all of its member nations and has also made the requirements much more stringent. For example, data breaches now have a strict reporting requirement of three days from the time an organization becomes aware of such an event. Fines are now very impactful, as GDPR states that even failure to report a breach can result in penalties of millions of Euros, up to 2 percent of a corporation's annual revenues. A willful or negligent violation of GDPR can result in a fine of 4 percent of corporate annual revenues.

4. Is there a grace period once GDPR hits?

GDPR goes into effect 25 May 2018, and there is apparently no grace period for companies doing business with European citizens.

5. What are three ways that a company can best prepare for GDPR?

From a data management and storage perspective, there are a few baseline prerequisites:

- Understand where data is stored, whether on-premises or cloud, and in what locations.
- Always use encryption for data, both at-rest and in flight. It is preferred to have user-managed encryption keys.
- Always track user access and security access, since breaches will happen. Make sure to keep the logs for future audits.

6. What are the benefits or any drawbacks you see for your customers after implementing GDPR? Will their user experience be any different?

Customers will see benefits of more security in several ways:

- Additional protection of their personal data, as it will force greater use of encryption hence reducing the chance of data leaks or exposure of identifiable data.
- The ability to choose whether personal data is maintained to a greater extent than before.
- As this ultimately this forces business to pay more attention to data as well as where and how it is stored, this can only help reduce risks.

7. In general, do you feel like your company is prepared? Has GDPR prep been a priority?

Scality is taking a lead in enabling solutions that can help companies manage data across multiple storage repositories and clouds. Multi-cloud data management will be a central part of the growing trend for companies to use cloud storage solutions, where "clouds" include corporate private clouds managed on-premises (and in many cases using object storage solutions such as the Scality RING as their foundation), plus external clouds such as AWS, Microsoft Azure and Google Cloud Platform. Scality's Zenko is focused on providing a comprehensive

multi-cloud data management solution that can help control where data is stored. Zenko can also perform searches that support GDPR requirements for data locality and sovereignty.

8. Should companies go beyond GDPR for extra safeguarding of information? Or is it very inclusive/extensive?

While GDPR is a strong step, it is best to combine these regulations with comprehensive security best practices that companies already take, for example, implementing multiple layers of network security, adding firewalls, installing virus detection and designing and using authentication and access control to storage systems.

Achieving GDPR Compliance with Scality

Right to Access

The GDPR enhances the rights of natural persons in many ways. It is important to ensure that the rights of data subjects are accommodated when processing their personal data.

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from a company's data controller confirmation as to whether personal data concerning them is being processed, where that processing takes place and for what purpose. Furthermore, upon request, the controller shall provide a copy of the data subject's personal data, free of charge, in an electronic format. This change is a dramatic shift toward data transparency and empowerment of data subjects.

Scality, with its RING S3 solution, can store user metadata linked to each object. That means additional information can be associated with objects when they are stored to help trace the source and the rights associated with said data. The Scality platform also allows metadata search to discover and retrieve this information without accessing the actual data.

Scality also provides flexible methods to create resource policies for access control of the stored data. By setting up the correct policies on the data, it can be protected as required by GDPR.

Scality key features:

- RING and Zenko S3 User Metadata (RING 6 or later, Zenko EE)
- RING and Zenko S3 IAM Policies (RING 6 or later, Zenko EE)
- Zenko Metadata Search (Zenko EE)

Right to be Forgotten

Also known as Data Erasure, the "right to be forgotten" entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer relevant to original processing purposes, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Scality allows you to maintain a data lifecycle policy based on many criteria. When required, Scality RING users can automatically delete the data following a specified legal retention period from the outset without the need to maintain a dedicated process to retrieve expired data. By creating a lifecycle expiration rule, users have the guarantee that the data will be deleted.

Scality key features:

- RING and Zenko S3 IAM Policies (RING 6 or later, Zenko EE)
- RING and Zenko S3 Tags (RING 6 or later, Zenko EE)
- RING and Zenko Lifecycle expiration (RING 7 or later, Zenko EE)

Privacy by Design

Privacy by Design as a concept has existed for years now, but is only now becoming part of a legal requirement with the GDPR. At its core, Privacy by Design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically — "The controller shall... implement appropriate technical and organizational measures... in an effective way... in order to meet the requirements of this Regulation and protect the rights of data subjects." Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing.

From design to integration, security is a key concern for Scality. Storing and managing data requires a strong architecture in terms of authentication, isolation and security.

Authentication: RING offers standard user authentication methods including integration with AD & LDAP services. Scality RING provides a VAULT system based on the AWS IAM protocol to store and secure every credential attached to a user. These credentials are encrypted in

the vault. The authentication protocol supports AWS authentication v4 system which enables:

- Verification of the identity of the requester. Authenticated requests require a signature create by using access keys (access Key ID, secret access key).
- In-transit data protection. In order to prevent tampering with a request while it is in transit, we use some of the request elements to calculate the request signature.
- Protect against reuse of the signed portions of the request. The signed portions of requests are valid within a period of time and for a specific payload.

Isolation: by design, the RING & Zenko feature multi-tenancy with strong isolation across tenants. From metadata to data, the architecture splits them both to prevent a user from accessing data or a piece of content that he does not own.

Security: the data could be encrypted at REST with a key stored in a third-party Vault.

Scality key features:

- RING and Zenko S3 User Metadata (RING 6 or later, Zenko EE)
- RING and Zenko S3 IAM Policies (RING 6 or later, Zenko EE)
- RING and Zenko S3 Auth v4 (RING 6 or later, Zenko EE)
- RING S3 Bucket encryption at rest (RING 6 or later)
- Zenko Metadata Search (Zenko EE)

Data breach notifications

Data controllers must report data breaches to the data protection authorities without undue delay and in any event within 72 hours of becoming aware of a data breach.

Scality can log each data access on the RING to help auditing and detecting any unusual activity on the storage. The RING audit log can trace every access to the supervisor to trace any access to accounts and volumes.

Scality key features:

- RING and Zenko S3 API (RING 6 or later, Zenko EE)

- RING and Zenko S3 User Metadata (RING 6 or later, Zenko EE)
- RING Audit log (RING 6 or later)

Data protection impact assessment (DPIA)

An organization may need to conduct a DPIA related to processing activities, and in some circumstances that DPIA may need to be filed with an EU supervisory authority.

To track every treatment of data, it would be tempting to track changes directly inside the object. However, to guarantee integrity and traceability, the metadata is immutable. It is not possible to update an object's metadata when an object is created. It is also not possible to update it when its data is processed by any particular treatment system.

Scality RING S3 Connector supports tags, which can be assigned to an object after its creation without altering the metadata or the data. A solution could be then to tag an object when a process is applied in order to maintain a trace of the treatment without altering the data.

Scality key features:

- RING and Zenko S3 API (RING 6 or later, Zenko EE)
- RING and Zenko S3 User Metadata (RING 6 or later, Zenko EE)
- RING and Zenko S3 Tags (RING 6 or later, Zenko EE)
- RING and Zenko S3 IAM Policies (RING 6 or later, Zenko EE)

Data processing agreement (DPA)

An organization may require a DPA that will meet the requirements of the GDPR, particularly if personal data is transferred outside the European Economic Area.

The issue here is to be able to know where the data is through all its applications. Since it is very difficult to update them to control and check if the data is inside or outside the European Economic Area, a solution could be to have a way to control location directly on the storage side.

Since Scality can tag the data without updating the object content, it is possible to add the origin of an object to trace location constraints directly within the storage system. Additionally, data policies can help you to prohibit inappropriate data movement such as keeping European data within the European Economic Area.

Scality key features:

- RING and Zenko S3 API (RING 6 or later, Zenko EE)
- RING and Zenko S3 User Metadata (RING 6 or later, Zenko EE)
- RING and Zenko S3 Tags (RING 6 or later, Zenko EE)
- RING and Zenko S3 IAM Policies (RING 6 or later, Zenko EE)

Conclusion

Globally, GDPR requires better traceability and control of an organization's data. Indeed companies need to secure it, retrieve it easily and maintain its lifecycle. These requirements fit well with Scality's vision which is to "Give Freedom & Control to People who Create Value with Data." Scality RING supports 500 million users and 1 trillion objects, proving Scality leadership in object and cloud storage by integrating features to manage and control data at scale.