> GDPR Compliance in Multi-cloud Environments

THALES

www.thalesesecurity.com

Understanding Your Responsibilities

The GDPR, which goes into effect in May 2018, aims to protect the privacy of EU citizens. Any such data that you hold across your cloud environment(s) is ultimately your responsibility and under your ownership, leaving you subject to potential scrutiny under the new mandates.

With the deadline approaching, it is critical to understand how your cloud services providers affect your compliance posture. Specifically, Article 32 of the GDPR requires organisations to take into account “the state of the art” and:

- Implement technical and organisational measures to ensure data security appropriate to the level of risk, including “pseudonymisation and encryption of personal data."
- Have in place "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
- Safeguard against the "unauthorised disclosure of, or access to, personal data."

Per Article 34, organisations must notify affected data subjects about a personal data breach “without undue delay.” This article also provides some relief to organisations, in that it states that such notification “shall not be required if…the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.”

Considering the potential fines of up to 4% of annual turnover, it is critical to understand how your CSPs affect your compliance with the GDPR.

Questions for Your CSPs

Considering the potential for large fines and the administrative burdens associated with a data breach, some of the critical questions to ask your CSPs include:

- **Can I control the keys encrypting my data?**

  Access to encryption keys provides access to any encrypted personal data, so it is preferable to control those keys yourself, when possible and practical.

- **Can you (the CSP) specifically encrypt database fields that contain personal data?**

  Focusing on just personal data would help you streamline your GDPR compliance efforts.

- **Does the encryption solution you offer include privileged user access controls to manage who has access to customer data?**

  Such user access controls will help you demonstrate ‘the ongoing confidentiality and integrity’ of personal data.

- **Do you offer security intelligence logs that show successful and unsuccessful attempts to access customer data?**

  These logs will help demonstrate evidence that you are ‘assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing’ of personal data.

- **Do you outsource any of your data storage?**

  Additional processors further complicate the GDPR calculus so it is essential to understand where your customer data will reside.

Data Encryption and Access Control in Multi-cloud Environments

In light of the challenges presented by the GDPR, and the ongoing transition to multi-cloud enterprise infrastructures, it is more essential than ever before to choose data protection that helps you adhere to compliance requirements and that can scale with your business needs.

Thales eSecurity partners with organisations worldwide to deliver comprehensive multi-cloud data security. Thales eSecurity enables customers to establish control over and trust in the integrity of multi-cloud data. The security of any personal data that you store in your cloud environments is critical given the high stakes associated with the GDPR.

Thales eSecurity offers comprehensive encryption solutions for multi-cloud workloads:

> ***"I think it makes sense for more large enterprises to adopt more than one cloud to make the best use of a variety of cloud services. ESG research shows that 75% of current public cloud infrastructure customers use multiple CSPs."***
>
> **~ Dan Conde, Analyst, Enterprise Strategy Group**

- From on-premises private clouds to SaaS providers, Vormetric Transparent Encryption, Application Encryption, Tokenization and Key Management as a Service all utilize the Vormetric Data Security Manager (DSM).

  A DSM deployed on your premises or as a virtual appliance in the cloud can manage encryption, keys and policies for any accessible server running Vormetric solutions.

- We help customers gain control of their encryption across public cloud providers such as Amazon, Microsoft and Google. Benefits include:
  - **No vendor lock-in.** Vormetric Encryption solutions work seamlessly across public CSPs for their data-at-rest storage offerings, in some cases more broadly than the vendor's proprietary encryption solution. The result is a single pane of glass for encryption, key and policy management. A single centralized solution also reduces training and operating costs.
  - **Data mobility.** A benefit of not using vendor-proprietary encryption and key management is that data can be moved from cloud to cloud *without being decrypted.* This can dramatically:
    - ✓ accelerate workload migration
    - ✓ eliminate costs of CPU cycles for decryption and data storage
    - ✓ keep data safe during migration

- Additionally, you can bring your own keys to multiple cloud providers.
  - IaaS/PaaS: Customers of Azure, AWS, or Google Cloud Platform can choose to utilize each vendor's proprietary encryption solution but maintain control of and access to data with Bring Your Own Key (BYOK) solutions supported by Thales nShield HSMs. A single HSM or HSM estate provides high-assurance key management for workloads across public CSPs.
  - SaaS: Customers of Salesforce.com and Microsoft Azure SaaS-based applications gain control of and access to data stored in SaaS clouds with Vormetric Key-Management-as-a-Service solutions.

Visit us at
www.thalesesecurity.com
to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Follow us on:

Americas – 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101-03, 41/F., Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com