

Analyst Research



Compliance Issues for Cloud-Based Data

ABI Research Blog

cpl.thalesgroup.com

THALES
Building a future we can all trust

Placing data in a third-party cloud can bring with it all kinds of new security issues. But just as importantly, there are aspects of regulatory compliance that enterprises need to address as well, and these can be highly challenging depending on the nature of the data and the location of the cloud infrastructure.

Regulatory Concerns in the Cloud

Data protection regulation is a cost- and effort-intensive endeavor. This is amplified when moving to a cloud platform, where enterprises hand over control of the hosting infrastructure to a third party. The issue of responsibility and, therefore, liability for data security are key challenges for enterprises in this scenario, especially because penalties for non-compliance can be financially significant.

Most data protection regulations impose prescriptive obligations on the data owner on how they manage data and implement security, including requiring notification to regulatory authorities in case of a breach. The difficulty in the Asia-Pacific region is that there is no unified regional instrument as in the European Union (EU) with the General Data Protection Regulation (GDPR). Instead, a host of various national instruments address data protection and privacy, each with its own distinctions and prerogative. This makes compliance requirements much more challenging for enterprises operating in various countries across the region, and even more difficult when also leveraging cloud services, which may not always be present in the same country of operation as the enterprise.

In addition, the issue of data sovereignty is an added complexity to that of data protection. Certain regulations in the Asia-Pacific region already include varying restrictions on cross-border transfers (Australia, Indonesia, China, Japan, Malaysia, the Philippines, Singapore, New Zealand, South Korea, Taiwan, and Thailand) and requirements for data localization (Australia, China, Vietnam, India, Indonesia, South Korea, Taiwan, and Thailand), all subject to different security guarantees.

Enterprises making use of cloud services in the region need to take into account the varying applicable regimes, ensuring the data stored both on-premises and in the cloud is compliant with local regulations; a double effort fraught with complexity. The issue then is one of understanding where responsibilities lie, and what level of compliance the cloud provider can guarantee.

Visibility & Control Issues for Enterprises

Ultimately, enterprises need to have some visibility into the functioning of cloud services and how data are stored there, in order to be fully compliant with applicable regulations. Are the data visible to or processed by the provider? Do the data ever leave the country? Are there any other third parties on the cloud platform that could be involved in deploying or maintaining the infrastructure? This requires a level of transparency from the cloud provider that is not always forthcoming, placing enterprises in a tricky position.

The risk due to the involvement of the cloud provider as a third party, and the loss of full data control, are both challenges that enterprises need to constantly be aware of in light of regulatory requirements, especially in the fluctuating environment of cloud services, where data could be backed up automatically in places or in a manner that results in non-compliance, and may be potentially (or inadvertently) exposed, or be temporarily unprotected. Further, the power imbalance between an enterprise and a cloud provider makes it even more difficult for enterprises to obtain visibility from the cloud provider and ensure that the data can be stored in a compliant way.

Enterprises clearly need a data governance strategy and an effective solution that is adapted to the challenges brought forward by the cloud; one that allows for visibility and, therefore, auditing that can satisfy data protection regulations.

About ABI Research

ABI Research is a global technology intelligence firm delivering actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today.

About Thales

Thales helps organizations protect sensitive data and software and deliver seamless digital experiences, with advanced encryption, identity and access management and software licensing solutions.

© 2023 ABI Research. Distributed with permission of ABI Research. Compliance Issues for Cloud-Based Data: October 2023.

© 2023 ABI Research. Used by permission. Disclaimer: Permission granted to reference, reprint or reissue ABI products is expressly not an endorsement of any kind for any company, product, or strategy. ABI Research is an independent producer of market analysis and insight and this ABI Research product is the result of objective research by ABI Research staff at the time of data collection. The information contained herein has been obtained from sources believed to be reliable. ABI Research disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular use.