Tackling the GDPR compliance conundrum with hybrid cloud

wipro

The most important change in data privacy regulation in 20 years is taking shape as European Union's General Data Protection Regulation (GDPR) came to effect from May 25, 2018.

A recent Deloitte GDPR benchmarking survey revealed that only 15% of organizations expect to be fully compliant with the new regulation by May 2018, with the majority instead targeting a risk-based, defensible position[1]. Approximately three-quarters of enterprise cloud services still lack key capabilities needed to ensure compliance with GDPR[2]. Though cloud-based data storage is often seen as being unsuitable for complying with GDPR cross-border restrictions, the truth is, several compliance advantages can be gained by moving EU data processing to the cloud. The real challenge however, lies in seamlessly managing a cloud environment and complying with GDPR simultaneously.

Let's deep dive into the implications for cloud transformation in the post-GDPR world and the value an expert IT services provider can add by driving long-term improvements aimed at mitigating current and future risks.

Technical and financial implications of GDPR on cloud computing

The journey to the cloud is inevitable and more and more enterprises are moving to the cloud to reap benefits such as flexibility, scalability and resource optimization, in a cost-effective manner. However, GDPR compliance in the cloud can be complex.

Technical implications: With data subjects given the right to correspond directly with a CSP or through an organization that uses the CSP, it becomes imperative to identify where the data lies and respond within the stipulated timelines. This is possible only if organizations fully understand the privacy rights and ensure privacy by design—where privacy is built into the cloud solution. How can businesses ensure this? To begin with, it's important to conduct an impact assessment aimed at identifying the gaps. This must be followed by an evaluation of how data is going to be protected by considering three aspects: where is the data stored, how is it processed and who accesses it.

Financial implications: The cost of non-compliance with GDPR far exceeds that of any previous regulation—it can attract penalties of up to 5% of a company's global turnover, besides resulting in reputational damage and loss of customer trust. Deploying the right resources with intimate knowledge of GDPR and ensuring training will be critical to preventing and quickly spotting violations.

The writing on the wall is clear: organizations simply cannot choose to be complacent when it comes to GDPR. But some challenges stand in their way.

GDPR and the cloud: What to watch out for

91% of organizations in a recent survey revealed they are concerned about how GDPR will impact cloud services[3]. While general privacy challenges are inherent to the cloud, GDPR brings in specific challenges including:

1. Determining data retention period in the cloud: GDPR mandates businesses to store personal data only for the period necessary to achieve its predefined purpose. Whether data is stored locally or in the cloud, it must be deleted effectively when the retention period expires. But with data being stored in multiple locations and subjected to multiple jurisdictions, identifying and managing diverse retention requirements can be a tall task. Further, deleting data completely requires businesses to

[1]Deloitte,Deloitte General Data Protection Regulation benchmarking survey, https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-readiness.html

[2]Beta News, Majority of Enterprise Cloud Services Still Not Ready for GDPR, Oct 2017 (accessed May 2018), https://betanews.com/2017/09/18/enterprise-cloud-services-gdpr-readiness/

[3]Scoop,GDPR, cloud and the concerns, issues and needs of IT decision-makers, https://www.i-scoop.eu/gdpr/gdpr-cloud-it-decision-makers/

Inefficient firewalls, legacy applications, and poor access controls become easy ways for hackers to get inside a company's data systems even if it resides in-house.

have clarity into how backups are secured by their cloud service providers (CSPs). Data storage in the cloud in the post-GDPR era ranks as one of the key concerns for over 93% of businesses[4].

2. Processing personal data outside the EU: GDPR mandates cloud providers to maintain appropriate safeguards, if adequacy decisions have not been made about the country where personal data resides. This means a multi-country cloud strategy must be developed to fulfil adequacy requirements and also ensure data portability (from one controller to another) for data subjects.

3. Managing risk: GDPR requires organizations to conduct a Data Protection Impact Assessment (DPIA) to determine any risks that may arise when using a CSP. Organizations must also possess the right to audit cloud providers and define an appropriate audit plan, complete with a control framework and privacy control measures.

4. Securing data privacy: Organizations typically do not have control over the CSPs' IT environment(s). However, they must understand the underlying technologies the CSP employs and monitor any changes/updates in their technology ecosystem. This can help determine the implications these technologies could have on the security safeguards and protection of the personal data stored and processed in the cloud.

How hybrid cloud can help organizations fast track GDPR compliance

One common misconception is that public cloud services, with data held by third parties on shared systems, can be potentially less secure and a bigger challenge to ensuring GDPR compliance than traditional in-house systems or a private cloud. The truth, however, is quite the opposite. Operating a private cloud puts the onus of total responsibility for ensuring security and compliance on organizations. This places greater strain on their internal IT, especially in cases of power outages/disasters, besides exposing businesses to greater chances of internal data theft. Inefficient firewalls, legacy applications, and poor access controls become easy ways for hackers to get inside a company's data systems even if it resides in-house.

Cloud providers, on the other hand, ensure that delivery of systems, tools and continuity plans are in place to make their cloud infrastructure safe and secure. Given the cut-throat competition among CSPs, innovative providers offer a value proposition around regulatory

[4]Scoop, GDPR, cloud and the concerns, issues and needs of IT decision-makers, https://www.i-scoop.eu/gdpr/gdpr-cloud-it-decision-makers/

compliance, data security, and privacy management. They typically store corporate data in a virtually secure facility, backed by multiple layers of physical security. Such a set-up is often absent or highly expensive to maintain, if businesses opt to manage their cloud infrastructure in-house.

Leveraging a hybrid cloud solution is the perfect answer to organizations' GDPR woes. It allows businesses to take advantage of the cost-effective public cloud for less sensitive, non-regulated data while storing sensitive information (that needs stringent GDPR compliance) on-premises. Hybrid cloud mitigates the risks associated with data residency regulations, giving organizations greater control over the availability, integrity, and security of their data.

Making the cloud and GDPR work in tandem: How a IT service provider adds value

IT service providers enable organizations to get the best of both worlds—unify different types of cloud, services, and enterprise data within a hybrid environment, enabling single pane of glass monitoring. Here are three unique ways in which organizations can benefit by partnering with an experienced service provider:

1. Identify the right cloud transformation approach: With GDPR going into effect end of May 2018, the challenge of deciding what goes where in a cloud environment has intensified. An expert service partner can sift through workloads to identify the best-fit hybrid cloud solution, depending on the type of industry, sensitivity of data, and applicable regulations.

2. Assess readiness of remote management center: Conducting an in-depth assessment of the cloud infrastructure readiness for GDPR compliance—datacenter facility, tools, applications, and workforce training is a key aspect where a service provider can add significant value. Skills gap is a daunting issue for most enterprises and addressing the advanced technical, GDPR specific compliance related challenges, can make it even harder for businesses. Partnering with a service provider ensures ready and scalable access to certified cloud and GDPR specialists across geographies.

3. Ensure continuous process improvements: Service providers and CSPs ensure software patching to bridge security gaps and mitigate risks from data breaches or non-compliance in a consistent, standardized fashion as compared to organizations running their own private cloud. Moreover, cloud transformation approach requires adoption of relevant IaaS, PaaS and SaaS services suiting to business in phased manner, so IT service provider plays significant role on consistent basis aligning transformation to GDPR requirement.

Accelerating GDPR readiness with hybrid cloud

Defining a new paradigm of information security is an enterprise imperative in light of the GDPR coming into effect in less than two weeks. Different organizations are in different phases of adoption. While some have already undergone transformation and are ready to capitalize on enhanced opportunities, many are still planning and strategizing. Regardless of where you are in the journey, leveraging hybrid cloud and the consultative approach of a service provider can help ensure that the right policies and solutions are in place for superior data practices and compliance.

About the author

Rajiv Kumar
Cloud Pre-Sales head,
Cloud & Infrastructure Services, Wipro Ltd.

Rajiv is the Head of Azure Cloud business at Wipro Limited. He has around 20 years of experience in the IT Industry and has represented Wipro in leading industry conferences and events on cloud, IT infrastructure and emerging technologies. He has played a key role in developing next-generation transformative offerings like Azure Stack and rapidly growing the cloud practice across global geographies. He is member of esteemed, Association of Enterprise Architects-AEA. He has many leading certification under his belt like TOGAF, Azure MCSD and AWS Solution Architect, etc. Reach out to him at **rajiv.kumar@wipro.com**

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/B&T/JUN-NOV2018