Satisfying regulations in the cloud

A friend of mine is a motorway traffic cop and I often enjoy her stories of people's excuses for speeding, but the one that comes up the most is: "I didn't see the speed limit sign." Unfortunately, not being aware of the law, is no excuse for not complying with it. The same, can be said for the cloud. The regulations are getting more and more complex and it falls on the head of IT to make sure your company is compliant.

I often see companies confusing governance with management, but they are very different beasts.

Managing the cloud is about maximizing processes and making sure objectives are met in full compliance with defined governance. Governance continuously monitors and audits rules and regulations, making sure they are met. But, having said that, it is important management and governance work together to optimize and secure cloud infrastructures.

Clients tell me that compliance paperwork is their biggest headache. Governance and compliance is a major issue for companies and starts the minute they decide to make a move to the cloud in an increasingly bewildering IT landscape. According to research firm IDC's GRC Software Market Forecast, regulatory compliance is becoming increasingly complex and corporate governance, risk and compliance initiatives placed under even greater scrutiny. The financial and reputational impact of high profile compliance and security breaches can't be underestimated. I'm therefore not surprised that risk management is at the top of most CEO's strategic agenda.

The General Data Protection Regulation (GDPR) has undoubtedly triggered urgent talks about governance and compliance in some companies. The European Union directive comes into force on 25 May 2018, replacing the Data Protection Act 1998. Created to give people more control over their own data, it comes with some sharp teeth and hefty fines for those who don't comply.

For further information go to: ***GDPR, Brexit and the shifting landscape for EU data regulations Reproduced with kind permission from 451 Research.***

For those who work in government or a highly regulated industry such as health or finance, data sovereignty and stringent security policies come with the territory. For others it is like sitting at base camp looking up at Everest and seeing the size of the challenge when the cloud part. According to a recent YouGov poll almost two-thirds of UK companies said they were unaware of the sanctions they could face after GDPR comes into force. Some of this I feel could be hiding their heads in the sand.

There are answers out there, as Microsoft was quick to point out at its Ignite conference in Florida.

Complying with complex regulatory requirements is a headache for any CIO. Azure has been designed to relieve some of these pain pints by allowing you to identify exactly what data you have and controlling who has access to it. This is paramount to meeting GDPR requirements. Azure, for example, enables you to manage users' identities and authorize access, including visibility and control over the security of your Azure resources.

Microsoft has recently rolled out a few offerings that should make compliance less complex. Azure Information Protection, a new offering in Azure Stack, for example, lets you define your critical data and who actually has access to it, which is crucial in GDPR compliance.

At Ignite recently, the wraps were taken off Azure Information Protection Scanner, developed to help protect significant on-premises data.

This will be a boon to companies preparing for GDPR.

In essence, you tell the scanner what locations you want scanned and the 'rules' you want to apply. The scanner then scans existing locations and continues to monitor them. This can help you identify data that meets specific regulations, such as GDPR, and choose which to migrate to the cloud and which to keep on-premises.

Of course, relocating sensitive cloud-based personal information to on premises will enable you to take the reins when it comes controlling your cloud data. Here Azure Stack comes into its own as it addresses the market for private cloud services with public cloud capabilities.

Whichever road to cloud you choose to take, it is essential that you put a firm governance and compliance strategy in place. My advice is to revisit it often. Otherwise you could find yourself sitting on the insecure ledge of a very rocky cliff.

About the author - Jason Tomlinson:

Jason Tomlinson, as Senior Director of Product Management for NTT Europe, is charged with ensuring that this global powerhouse remains competitive in the IT services landscape by bringing new solutions to market that resonate with a demanding client base.

He is drawing on his rich experience spanning over a decade in ICT to deliver in this strategic position. Jason has built a wealth of knowledge in both ICT systems and how they impact on business outcomes from his foundational roles while rising through the ranks of NTTE.

Leveraging this extensive experience, he is well placed as a thought leader on the topics of digital disruption, automation and the future of cloud technologies.