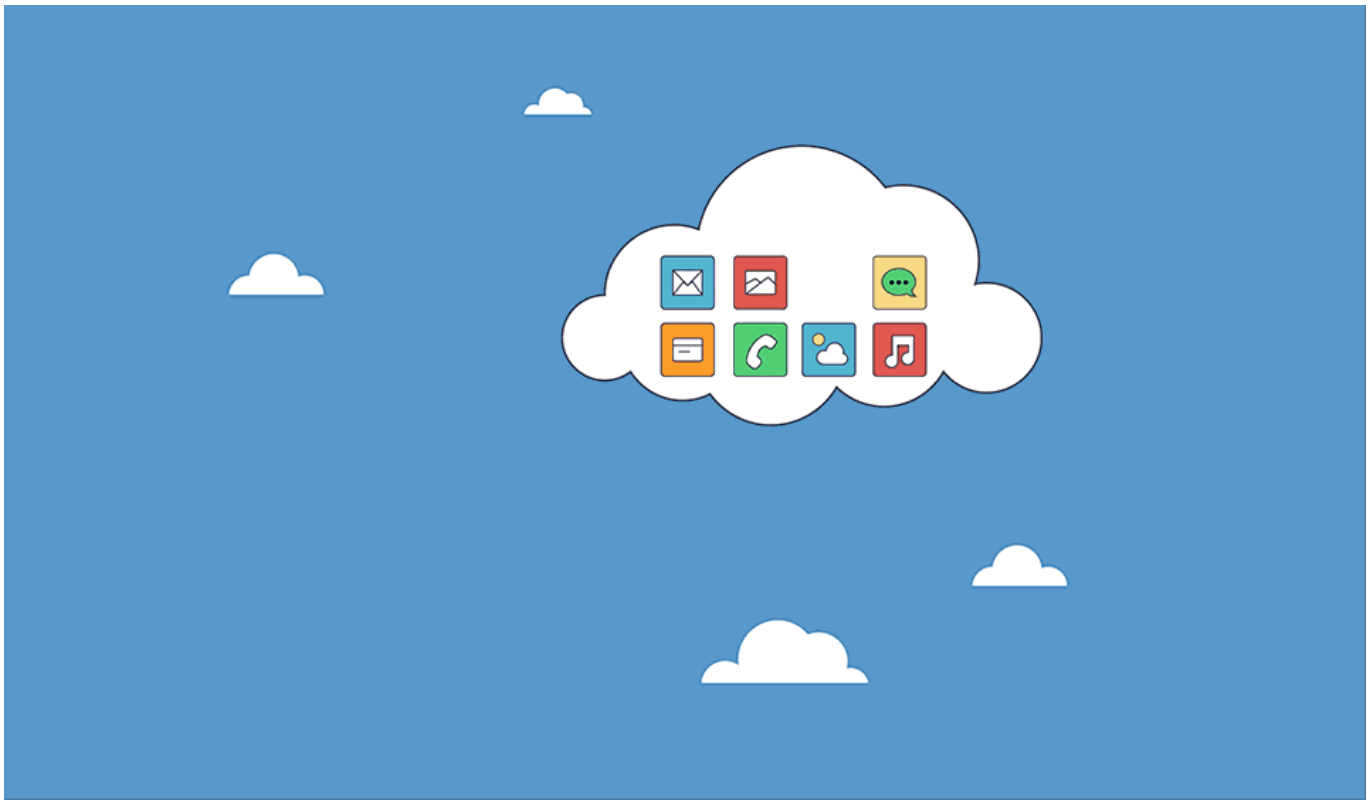
Using cloud storage? You may be in breach of GDPR



Posted on Tuesday, August 29, 2017

Much has already been written about the General Data Protection Act (GDPR), Europe's new regulations for governing the use of citizen's personal data. Even more has been said about the potentially enormous fines that will be levied on companies which breach the Act (up to 4% of *global* turnover!).

But much less attention has been given to cloud services once the GDPR comes into effect. Because, worryingly, cloud storage services could be in breach of the GDPR.

Personal data must not be shared

The heart of the problem lies in the proviso that personal data must not be shared outside your company, nor used for purposes other than those laid out in your data protection statement. Public cloud services may, because of their design, be in breach of those rules.

Cloud service providers have certainly improved security, preventing leakage of data between accounts for instance. But public cloud does allow virtually anyone to access anything. Should a third party gain access to the data you store in the cloud, who is responsible? You, because your users choose weak passwords, or the cloud provider for failing to prevent a hacking?

The European courts are interested in the data leakage – not how it happened. So you and your cloud provider must

allocate responsibility *before* a breach happens. In fact, that agreement needs to be in place before GDPR comes into force.

The Google problem

Artificial intelligence is now being used to help service users surface context-relevant data more quickly. Google's G Suite customers already benefit from data mining technologies that scan email for important data, automatically inserting appointments into diaries for instance.

There is a problem however. In theory, no one at Google is accessing this information as it is scanned – but the fact that a third party *is* reading potentially confidential messages, that activity falls foul of the GDPR. Your customers gave *you* permission to access their personal data – not Google.

It may be that your business may need to change the way it uses cloud services – and quickly.

An unlikely data centre renaissance?

Ironically, the best way to ensure your data is not being used/accessed by third parties is through the use of your own on-site data centres. Because you have full control of security and access rights, you can better protect your customers.

As the GDPR activation date inches closer, it may be that your organisation needs to delay further cloud rollouts to ensure you are 100% compliant. And if the cloud migration is being driven by your need to retire post-warranty arrays, you may need to consider the use of a third party support provider in the interim.

To learn more about redeploying your existing data storage arrays – including post-warranty assets - please get in touch.