HERBERT SMITH FREEHILLS

BLUE SKY THINKING: FCA PUBLISHES CLOUD OUTSOURCING GUIDANCE

06 September 2016 | Europe
Legal Briefings

In July 2016, the FCA published its final guidance for financial service firms outsourcing to the "cloud" and other third party IT services (the "**Guidance**"). The guidance confirms that it is possible for firms to outsource to the cloud, including the public cloud, in a manner that is compliant with FCA rules. As such, it is likely to be welcomed by financial services organisations and service providers alike. However, it is not all plain sailing, and firms will need to consider their regulatory compliance carefully in consultation with the guidance before embarking on any cloud outsourcing.

This briefing sets out some of the key issues covered in the Guidance which firms and service providers will need to consider in the context of any financial services outsourcing to the cloud.

STATUS OF THE GUIDANCE

The Guidance is not legally binding and firms will need to continue to comply with their regulatory obligations with respect to outsourcing, as contained in the Senior Management Arrangements, Systems and Controls sourcebook ("**SYSC**"). However, the FCA has confirmed that it believes that compliance with the Guidance will generally indicate compliance with the FCA outsourcing requirements.

IDENTIFYING THE SUPPLY CHAIN

In its original proposed guidance, the FCA had included a requirement that firms identify all the service providers in the supply chain and ensure that the requirements on the firm can be complied with throughout the supply chain. Many respondents to the original consultation noted that this requirement was impractical and unduly burdensome in an environment where supply chains are often large and complex. As a result, the FCA have slightly amended their position in the Guidance to provide that firms are only required to identify service providers in the supply chain providing services relating to regulated activity (i.e. not necessarily all providers in the supply chain).

A similar approach has been taken in the Guidance to subcontracts. Rather than requiring firms to review all subcontracting arrangements (as was proposed in the original version of the guidance), the Guidance limits this obligation to arrangements relevant to the regulated activity.

BREACH NOTIFICATION

The Guidance obliges firms to require prompt and appropriately detailed notification of any breaches or other relevant events arising, including the invocation of business recovery arrangements. In the responses to the original consultation, a number of firms had suggested that a threshold for breach notification should be stipulated. However, the FCA have suggested that the wording in the Guidance gives firms flexibility to consider and agree with service providers what constitutes a breach (or other relevant event) in the context of the service being provided.

Firms should also note the data breach notification requirements in the EU General Data Protection Regulation which will apply from 25 May 2018. This legislation will require data controllers to notify the Information Commissioner in the UK of any data breaches within 72 hours of becoming aware of the same, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Firms may therefore wish to consider this new regulatory requirement when agreeing with service providers about the notification of breaches in the context of the Guidance.

DATA LOCATION

In its original proposed guidance, the FCA had suggested that firms looking to use cloud services would need to have "choice and control regarding the jurisdiction in which their data is stored, processed and managed". Both service providers and firms alike raised concerns about this requirement in the consultation, arguing that choice and control was impractical and may stifle service provider innovation. The FCA responded to state that it wished to ensure that firms are able to determine in which jurisdictions their data are held, whilst recognising that many service providers are not able to allow firms full control of this. The Guidance therefore provides that firms must agree a data residency policy with service providers, which sets out the jurisdictions where their data can be stored, processed and managed. Service providers would then be free to process data in any of the jurisdictions agreed in the data residency policy.

This requirement should also help firms with their data protection compliance. The Data Protection Act in the UK restricts the ability of data controller organisations to transfer data outside of the EEA. By agreeing a data residency policy with service providers, firms will have oversight of the jurisdictions in which their data is being processed, to enable them to put appropriate data protection compliance mechanisms in place.

ACCESS TO DATA CENTRES

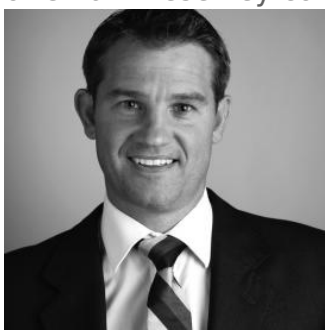
The Guidance provides that firms should be able to request an onsite visit to relevant business premises. It further reminds firms that SYSC 8 requires them to have "effective access to data related to the outsourced activities, as well as to the business premises of the service provider". A number of respondents to the original consultation had noted that access to data centres in particular could be impractical, raising significant security concerns. In response, the FCA has noted in the Guidance that it views "business premises" as a broad term which may include head offices and operations centres, but does not necessarily include data centres.

Unfortunately, this appears to be an area where firms may struggle to balance commercial agreement with regulatory compliance. Although the Guidance appears to acknowledge that access to data centres may sometimes not be commercially possible, it does not rule out the fact that SYSC 8 regulation requires access to business premises, which may include data centres.

To view a copy of the Guidance, please click **here**.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



NICK PANTLIN
PARTNER, HEAD OF TMT & DIGITAL UK & EUROPE, LONDON
+44 20 7466 2570
Nick.Pantlin@hsf.com

MIRIAM EVERETT
PARTNER, LONDON
+44 20 7466 2378
Miriam.Everett@hsf.com

DAVID COULLING
PARTNER, LONDON
+44 20 7466 2442
David.Coulling@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.
