Butter and Chicken Drumsticks

Cogitations on the implications of the National Security and Investment Bill for data centres

December 2020

The National Security and Investment Bill was published on 11 November 2020 and has far-reaching implications for data centre operators, customers, developers and investors with interests in the UK market. Although it is not yet law, once the regime is in force it will have retrospective powers on all transactions uncompleted by 12 November 2020.

Simplistically speaking, the Bill extends the government's power to scrutinise acquisitions, mergers and other transactions in the interests of national security. Hitherto this power has applied to a very limited range of activities and the UK's attitude to inward investment has been liberal – some say too liberal- which has helped make us an attractive destination for FDI. This Bill aligns us more closely with other countries like Germany and the USA. The government intends to capture any transactions that could give unfriendly entities access to sensitive data or data that could pose a potential threat to national security.

This is not new – in July 2018 Government issued a White Paper proposing updates to our FDI regime, but this bill imposes much more significant changes than were set out in 2018. The 2020 Bill signals a significant change of stance and identifies 17 sectors where transactions will be subject to increased government control. These must be notified in advance to the Department for Business, Energy and Industrial Strategy (BEIS) so that they can be subjected to scrutiny by a specialist team. The government has 30 days to decide whether or not to "call in" the transaction. If so, the scrutiny process can be extended by a further 75 days. Extensive information on both acquirers and investors is required – which some observers think may create discomfort around commercial confidentiality. There is no minimum transaction value.

While the Bill took effect immediately upon publication, the definitions of the 17 sectors within its new scope were subject to consultation. So which sectors are now in line for scrutiny? It will be no surprise that, along with obvious candidates like military, transport, space and energy the focus is primarily on digital technology, from quantum computing and AI to cryptography and hardware. Data centres have not escaped attention and are explicitly covered under Data Infrastructure (No. 10 on the list). The listing is supported by a draft legal definition which is currently being revised following consultation with the sector.

While the stated intent of the legislation is only to capture those transactions that could pose a genuine risk to national security, the current definition actually sets the scope very broadly. With respect to data centres, the proposals capture any entity with enough operational control to access or compromise sensitive data. Anyone acquiring such entities will need to notify Government of the transaction. This suggests that those able (in theory) to disable IT functions by interfering with infrastructure elements like power or connectivity would be captured, which widens the net significantly. So colocation providers and developers are presumably in scope, if the data they house is deemed sensitive. So are contractors and consultants working in the data centre space. Therefore anyone wishing to acquire a facilities management business in order to broaden their portfolio of

service offerings within the data centre space might have to notify BEIS of this deal. On the plus side it looks like landlords with no operational remit are unlikely to be captured.

So how does this apply in a colocation environment? For a simple comparison, think of a cold storage facility holding butter for Marks and Spencer and providing temperature controlled facilities for a number of customers to specific standards. Each customer has their own secure area in the warehouse. The cold storage operator doesn't have access to the butter. Yes, they could compromise the butter by melting it if they switch off the chillers but they can't inject Sarin into each pack or steal it and sell it themselves from the back door.

So is government just trying to control who accesses sensitive data or do they really want to control anyone who can compromise sensitive data? It seems to be both. This is troublesome for operators because they cannot resort to existing operational, physical and contractual controls on data security to demonstrate that they cannot access sensitive data. Nor can they use existing frameworks like GDPR that set out roles and liabilities of data controllers and processors. Focusing on the potential to disrupt, destroy or block legitimate access to data is a step change in policy and widens the impact hugely.

There is a second problem for commercial operators: how do they know if their facility hosts critical or sensitive data as defined in the Bill? And what is sensitive data anyway? So, going back to butter, Marks and Spencer know exactly what kind of butter they have in their cold store but the cold storage facility provider doesn't: they don't know whether it is Lurpak or M&S own brand – or chicken drumsticks for that matter. And which type matters? Just the Lurpak or all of it? In the real world, the likelihood is that many transactions will be notified unnecessarily as a precautionary measure. And the issues don't end here.

So what are the implications for a sector characterised by consolidation, M&A, rapid investment flows and extremely short development cycles? At techUK we will be examining those closely over the coming months, and we look forward to working with our dedicated team within DCMS to review further iterations of the definition if called for. Broadly, however data centre transactions look set to be subject to at least some degree of uncertainty, delay and cost.