GUIDE
CLEAR THINKING

ukcloud

In association with UKCloud

The Brexit General Election: A digital cloud on the horizon?

Spring 2017

In association with UKCloud

Preface

This report highlights the significant risks and opportunities political parties should consider as they set out their policies on public sector procurement. The next Government's approach to public sector spending will have a major impact on the UK economy after the general election, in the run-up to Brexit, and after the UK leaves the EU, so it is vital to get these policies right.

The GUIDE Consultancy

We are a political intelligence agency, advising clients on how they will be affected by political change. The GUIDE team is made up of staff drawn from different fields, including Westminster, Whitehall, the intelligence community, political research and public affairs. We are 'poachers-turned-gamekeepers' trying to describe current political issues and help clients to navigate them.

To find out more, please visit www.theguideconsultancy.co.uk

What is the 'cloud'?

This report includes references to the digital 'cloud', which will play an increasingly important role in public sector procurement after the general election – and it will be the source of some of the biggest risks and opportunities facing the next Government. Using the cloud is essentially a way for Government Departments and other public bodies to subcontract a huge amount of the computing requirements and data storage to a company with specialist facilities.

The cloud is made up of a series of physical data servers, often owned by private companies. These companies provide the Government with access to their cloud servers for a fee. These servers are in a series of locations and, depending on which company is providing the cloud services, can be based either in the UK or in other countries. Public bodies pay to store data in the cloud and access that data via the internet or via government networks. Using the cloud allows public sector organisations to reduce the cost of their own on-site servers, as long as sufficient security measures are in place to keep their data safe.

GUIDE CLEAR THINKING

ukcloud

In association with UKCloud

Executive summary

The general election has been called with a view to improving the UK's position regarding Brexit. The Government's ability to secure the best outcome from the Brexit negotiations will rely – to a surprising extent – on how it chooses to spend more than £240bn a year with private sector suppliers.

Government procurement policies rarely make the front page, but they should be given careful consideration in this general election. If the next Government commits to spending money wisely, especially where public sector procurement is becoming increasingly digital, our negotiating position in Brexit talks would be strengthened and the UK would be in line for an economic boost after Brexit takes place. The Government's approach to digital procurement is important to Brexit in three ways.

First, it could help mitigate the economic effects of state aid rules that will apply post-Brexit, regardless of whether we have a 'good deal' or 'no deal'.

Second, it could reduce the risk of capital flight in industries that may be hardest hit by Brexit, encouraging businesses to stay here in the UK.

And third, it could allow private companies to make a greater investment in the UK's post-Brexit economy, developing our workforce, local communities and expanding our tax base.

If digital procurement is given the right kind of boost after June, so that it achieves a really transformative effect, we could see significant economic growth in the UK's tech industries, with private sector suppliers helping to address some of the likely post-Brexit challenges, such as new customs arrangements and the need for 'frictionless trade'.

However, the next Government faces significant risks when it assumes office in June. A lack of commitment to the Open Government agenda could lead to an over-reliance on a few very large foreign-owned tech companies. These companies may base valuable parts of their business overseas and under the jurisdiction of foreign governments, while keeping sales and marketing teams in the UK. This could reduce the cyber security of public data held by the UK Government. It would also be to the detriment of UK-based tech companies – and especially innovative SMEs.

This raises questions about how public spending can be used to nurture companies paying Corporation Tax in the UK and foster digital skills across the UK workforce. Similarly, by considering how to extend social value goals in digital procurement, the next Government could avoid the risk of unnecessarily limiting what it can achieve in terms of building up the UK workforce, as it delivers social value procurement in partnership with its suppliers.

Attempts to address these risks in digital procurement have already been made in the public sector, but more needs to be done. Given the huge and growing array of public services and economic output that is reliant on digital procurement policies, the next Government must be even more cyber-secure and cyber-effective.

To this end, many people would welcome new protections for Government data stored in UK-based data centres, as well as the repatriation of particularly sensitive public data that is stored in cloud servers in other countries, where there may be a different approach to cyber security and where foreign regulators may have different rules on data security and access to data. A broader digital supplier base, with more innovative solutions delivered by tech SMEs, would also help de-risk public sector procurement – with an additional benefit being a boost to the Treasury's coffers from companies that pay Corporation Tax in the UK.

Commitments to take exactly these steps have previously been made by politicians, Civil Servants and regulators alike. The 2017 general election provides an opportunity for the political parties to set out how they intend to deliver on those commitments, build on the Government's approach to digital procurement, and significantly strengthen the UK's position in the run up to Brexit.

Greig Baker
Chief Executive, GUIDE

In association with UKCloud

The general election and Brexit: Why does procurement matter?

Procurement policy is often – and sometimes fairly – seen as dry and technocratic. In this election and in the Brexit talks to come, it could be anything but. In fact, the Government's approach to procurement after June will have a material effect on the economic outcome of Brexit, so it should be carefully considered by all of the political parties in the coming general election campaign.

Public sector procurement will be key to delivering a successful Brexit for three reasons:

ONE: It will help mitigate state aid rules, regardless of whether there is a 'good deal' or 'no deal'.

TWO: It will encourage investment in sectors at risk of capital flight by helping to create a more benign environment for the companies that are most fearful of Brexit.

THREE: It can be used to persuade private companies to pay for and deliver specific social policies, in addition to those policies being delivered by the Government directly.

Mitigating state aid rules

Theresa May has called a general election for 8th June with the explicit intention of securing a stronger mandate in her Brexit negotiations. The outcome of those negotiations will have a measurable impact on the UK economy and, as a result, there will continue to be a huge amount of speculation about the shape of any prospective trade deal between the UK and the EU – or, indeed, whether any deal can be reached at all.

However, almost regardless of the outcome of the Brexit negotiations, some factors affecting the Government's economic policy will remain constant. For example, EU restrictions on state aid are already widely recognised and we expect they would continue to be applied in the UK under most versions of a comprehensive trade deal with the EU27. Less widely noted, broadly similar restrictions on state aid would also apply under a WTO 'no deal' scenario, as any WTO member (including the EU) would be able to bring a complaint against a UK Government that began awarding major industry-specific subsidies or that sought to intervene to support an individual company.

> ***"The digital economy will be fundamental to a successful Brexit"***
>
> **Simon Hansford, CEO, UKCloud**

This makes the next Government's approach to public sector procurement all the more important, as procurement decisions are more likely to be beyond the purview of any deal (or WTO rules in the event of no deal). The Government will be able to use public sector procurement (and especially modern digital procurement) to support the UK economy and counter any potentially negative economic pressures we may face post-Brexit.

Encouraging investment and avoiding capital flight

The National Audit Office estimates that the Government (excluding local government) procures around £240bn of goods and services from private and voluntary sector providers each year. Clearly, such an immense amount of money plays a significant role in shaping the kind of goods and services that suppliers provide, with a corresponding influence on the investments they make to meet the needs of non-Governmental customers, too. In other words, Government spending influences what the UK economy sells inside and outside of Whitehall.

To date, the Government has been astute in using its online procurement policy to encourage private sector suppliers to make substantial investments in new technology. For example, the Government's *Cyber Essentials* scheme started life with an exclusive focus on suppliers to the public sector – it has now been adopted and promoted by companies like Barclays, BT, Vodafone, Astra Zeneca and Airbus, who are encouraging their own suppliers to invest in digital to meet *Cyber Essentials* standards, too.

By encouraging private companies to invest more heavily in UK-based tech, the Government will dramatically improve its ability to support the UK economy post-Brexit, should it need to do so. This view is supported across the business community – Simon Hansford, CEO of UKCloud (winners of *The Sunday Times Tech Track 100*) maintains that "the UK's flourishing digital economy will be fundamental to a successful Brexit, and wider economic stability and growth".

Moreover, this ability will be most easily applied (and it will be most demonstrably valuable) in sectors where there could be the highest risk of capital flight if new trade barriers are erected between the UK and the EU. This means the Government will be better able to persuade companies that might be minded to leave the

"Digital spending by Government could encourage companies at risk of capital flight to stay here post-Brexit"

The GUIDE Consultancy

UK post-Brexit that they should remain here by making their commercial environment more benign.

For example, a future Government will be able to offer benefits to private companies that invest in UK-based tech. These benefits could include tax relief on research and development costs, investment support via co-owned tech incubators, and access to publicly funded cyber security protection. In fact, it is encouraging to see that all of these things are already starting to happen, with more than £270m used to launch the Industrial Strategy Challenge Fund.

Economists with concerns about the impact of Brexit should take some cheer when they see where these benefits will be most keenly felt. While these measures will ostensibly be available across all sectors of the UK economy – which means they will stay on the right side of industry-specific state aid restrictions – they will offer the greatest benefit to industries that have voiced concern about the impact of Brexit on their future prospects. So, for instance, automotive industry worries about tariffs may be mitigated by tax relief on investment in driverless cars, while financial sector concerns about passporting might be countered by improved cyber security for fintech.

Even in instances where the Government is not directly commissioning goods or services, the size of its overall digital procurement spend means it can influence what the market produces, how it provides digital services, and the shape of the regulatory environment designed to protect and encourage investment in sectors that might be 'hit' by Brexit.

Delivering social value

Public sector procurement is set to have a growing economic and social impact in the run-up to Brexit and after we leave the EU. The next Government can build on that by grasping the opportunity to encourage suppliers to further support social policy goals as they deliver on their contracts. Many companies that supply the public sector already help deliver objectives beyond their core services – with promises to invest in social value programmes like apprenticeships, skills training and promoting workforce diversity commonly included in bids for otherwise distinct goods and services.

In March of this year, the Cabinet Office also confirmed that DCMS "has recently conducted a review to assess the impact of the Public Services (Social Value) Act on public procurement" and that "this review will be

> ***"We will be placing social value at the heart of procurement"***
>
> **Crown Commercial Service**

published in due course". If this review could be published as the general election campaign begins, it would help inform the political debate on how digital procurement can contribute to an economically successful Brexit by encouraging private sector firms to deliver more social value outcomes.

In the meantime, the Civil Service remains committed to promoting social value through procurement. As recently as 18th April this year (the day Theresa May called for a general election), the Crown Commercial Service announced it would be "placing social value at the heart of procurement" in line with the Public Services (Social Value) Act 2012, and based on the *Procurement for Growth* scorecard that it promoted in October 2016. CCS even said it would be "reviewing *current deals* [emphasis added] to identify social value opportunities" through individual procurement frameworks, like *Technology Products 2*. This suggests an appetite for adding new social value requirements to contracts that have already been signed off.

In some instances, this could be good news and it would be explicitly welcomed by suppliers. UKCloud's CEO Simon Hansford confirms that "given government's massive spending power and transformation agenda, the UK really needs to have social value embedded in the DNA of its digital purchasing". However, so far, researchers have struggled to identify clear examples of social value criteria being applied consistently in public sector procurement contracts secured through the Government's digital cloud platforms (e.g. G-Cloud), despite the increasing prevalence of these contracts.

When a Government Department signs any contract outside the cloud that is worth more than £10m or that will take more than a year to deliver, it must explicitly consider the social value of that contract. Social value criteria that must be considered include the potential to improve people's digital skills, users' digital confidence and the public's understanding of why using the internet can be relevant and helpful. It is ironic then that if a Government Department must consider the impact on digital skills when signing a traditional procurement contract, the same Government Department can sign another procurement contract *through a digital platform* without appearing to give the same level of consideration to that contract's impact on digital skills or other social value goals.

> ***"The UK really needs to have social value embedded in digital purchasing"***
>
> **Simon Hansford, CEO, UKCloud**

Significant progress has been made in delivering digital social value through *traditional* public sector procurement: around 200,000 adults are supported with free digital skills sessions each year; the Digital

Skills Partnership has been expanded; and public bodies are becoming digital 'demand aggregators', improving the business case for the broadband universal service obligation. It makes sense to use *digital procurement* to support these social value programmes, too.

After June, the next Government may wish to explore ways of ensuring public bodies can deliver social value goals through their digital procurement decisions, in the same way they have done with other contracts signed outside the cloud in the past. This could include providing clear guidance to public sector buyers using G-Cloud, for example, regarding how and when to apply social value criteria in their procurement decisions.

Brexit Britain needs tech

In most post-Brexit scenarios, the future looks bright for private companies that can supply the Government's digital procurement needs. Indeed, it may be no exaggeration to say that the Government's ability to make a success of Brexit will depend heavily on its digital procurement prowess.

Some of the most daunting challenges of Brexit could be effectively addressed through savvy use of online procurement by the Government to buy and apply new technological solutions.

Customs arrangements, for example, are likely to rely on new IT systems and processes that can track goods and travellers without the need for costly delays at the border and unnecessary bureaucracy beyond it. Similarly, there is speculation that HMRC will need to dramatically increase the capacity of its customs filing system to record international trade as it happens and ensure that 'frictionless' trade is possible even if it can be agreed between the UK and EU27.

The Government Digital Service has reinforced the expectation that post-Brexit there will be a greater reliance on tech solutions by suggesting that spending controls on Government IT projects could and should be relaxed to meet a growing demand for them – especially as various legacy IT systems fall due for updating at the same time.

"We must make the UK one of the safest places in the world to do business online"

National Cyber Security Strategy

The new Government must tread carefully

If the next Government is to exploit the opportunities provided by a strategic digital procurement

programme, it will need to mitigate two significant risks. First, it will be necessary to build on measures to protect Government data stored in cloud servers if they are based outside the UK, or to repatriate especially sensitive data to UK shores and to cloud servers exclusively under UK control. This could be done by working with UK-based tech companies whose approach to data security is not subject to foreign jurisdictions. Second, the next Government should consider redoubling efforts to award a greater proportion of digital public sector contracts by value to SMEs (which are commonly also UK-based companies) as this would help to diversify – and de-risk – the Government's supplier base.

Thankfully, these issues appear to be recognised by both the incumbent Government and MPs from across the political spectrum working in various Parliamentary Select Committees.

Some Government Departments have opted to use cloud servers owned by overseas companies that are subject to another country's jurisdiction (including, for example, the ability of foreign governments to access the data in cloud servers) but politicians, Civil Servants and regulators do acknowledge the importance of UK-based digital security. For instance, the Government's recent National Cyber Security Strategy explicitly recognises the vital importance of the physical location of data storage and processing, such as cloud services. Indeed, it goes so far as to say that new measures "to keep the UK's cyberspace safe are crucial to the future of the UK's economy" and it reiterates the Government's "aim to make the UK one of the safest places in the world to do business online".

In the same Government paper, the Chancellor explained that "Britain is already an acknowledged global leader in cyber security, but we must now keep up with the scale and pace of the threats we face" and Cabinet Office Minister Ben Gummer went further, saying the UK "cannot remain secure and prosperous without securing itself in cyberspace".

Similarly, the UK's first ever Director General for Digital has an explicit remit to "create an innovation-friendly and cyber-secure country" and the UK's first National Technology Advisor argues that "it's not unreasonable that people want to keep data in the UK. Citizens want to trust that their Government – and companies – is holding their data securely." In a Written Answer in Parliament on 30th March 2017, Digital Minister Matt Hancock confirmed that "the UK's data centre industry will play an important role in our ambition to grow the digital sector's contribution to the UK economy to £200bn by 2025 [and] we will support the continued growth of the UK data centre industry".

> ***"The UK cannot remain secure and prosperous without securing itself in cyberspace"***
>
> **Rt Hon Ben Gummer MP, Cabinet Office Minister**

The Government Digital Service has also started to explain how the need for territorial security should be considered when using G-Cloud suppliers that are helping to deliver public sector contracts. For example, in its digital marketplace supplier guidance, GDS states that "G-Cloud suppliers must include information [on] how secure their services are [and] where they store their data".

This guidance is based in part on fairly prosaic practical concerns. In its recently published Strategic Suppliers risk assessment, the Government points to the additional administrative burden of having to scour, verify and rely upon publicly available information on the security measures of digital suppliers based in other countries, as well as those companies working in the UK but still subject to foreign jurisdictions, compared to the private and trusted information given to Government Departments by UK-based regulators assessing the security measures adopted by cloud providers with facilities here that are exclusively regulated by UK authorities.

This is not controversial: it seems to be logical that the Government finds it easier to fulfil each of its own '14 cloud security principles' when assessing the security measures designed, controlled and implemented in the UK, rather than gauging whether or not similar measures are in place at different cloud facilities around the world – or indeed, at UK-based facilities owned by companies that are subject to a foreign government's jurisdiction.

The Information Commissioner's Office has set out how Government Departments and other public bodies should assess the risk of using cloud servers if they do decide to use servers that are based outside of the UK. The ICO says that "cloud customers should ask a potential cloud provider for a list of countries where data is likely to be processed and for information relating to the safeguards in place there".

The ICO has also stressed that "the obligations of the [public sector] cloud customer as a data controller will not end once a cloud provider is chosen", so the commissioning public sector body should "assess the security measures used by a data processor by inspecting their premises". This kind of inspection should consider whether premises are secure from both unwanted *physical* access and *virtual* access. Illicit physical access would occur if someone broke into a facility – but unwanted virtual access could include a foreign government insisting on access to data about UK citizens, even if that data is stored in a UK-based facility or secure Government network, because the company providing the cloud servers may be also subject to another country's cyber jurisdiction.

This kind of focus on cyber security, jurisdiction and who can access data managed by foreign companies is at the heart of some of the recent debates between Government and industry, for instance around 'Safe Harbor', 'Privacy Shield', 'Rule 41' and the US Patriot Act.

The ICO also says that Government Departments should "inform the end users of the cloud service about the processing arrangements that the controller has put in place" – which means the Government should make it clear to members of the public when they are using public services that require their personal data to be stored or processed in another country. Similarly, there is a duty on Government Departments to tell members of the public when their data in UK-based cloud facilities is also subject to the jurisdiction of a foreign government, by virtue of where the company providing the cloud is legally headquartered.

There will always be digital security threats and sometimes tech advances will outstrip the Government's ability to police them – as we have seen with end-to-end encryption. But if future Governments will have to work hard to know *how* they can verify the digital security of their suppliers, there may at least be advantages in knowing *where* those digital security checks can take place.

De-risking digital

Even with the best UK-based security measures to protect the digital services Government buys to store and manage sensitive data, threats will always exist. This means the next Government should take care to de-risk public sector digital procurement as far as possible. One important way of doing that will be to ensure there is a diverse supplier base that fosters innovation in digital security and avoids over-reliance on a few large-scale providers.

The National Audit Office has applauded efforts to take some steps in this direction. In March 2017, the NAO explained that "GDS has worked with the Crown Commercial Service to diversify the supplier base [and] to improve contracting with SMEs". Business leaders are reassured by these efforts – as Simon Hansford says, "UK SMEs are the powerhouse of the UK's digital economy, and government recognises this".

However, the NAO also warned that "94% of government procurement with digital and technology suppliers continues to be with large enterprises", so there is still more to be done to secure a truly diverse and de-risked digital supplier base. Hopefully the

> ***"The obligations of the cloud customer will not end once a cloud provider is chosen"***
>
> **Information Commissioner's Office**

incoming Government will pick up on the work of the Connell Small Business Research Initiative review, which was designed to encourage public sector procurement of new tech from a wider range of SMEs.

The importance of encouraging SMEs that can help meet the public sector's digital needs is becoming more widely recognised. Before June's general election was announced, for example, HMRC showed it had begun to assess the potential for the Government becoming over-reliant on larger enterprises with initiatives like the Large Business Risk Review, which was due to include a consultation ahead of the summer recess this year.

Large digital enterprises are not inherently less secure than those SMEs that already have accreditation certificates, CSA Star certification, and that meet ISO27001 and ISO28001. Larger companies have the resources and expertise to invest in digital security measures and are equally capable of delivering innovative solutions to counter cyber threats. However, if the public sector relies on a small number of companies – whatever their size – to deliver most of its digital procurement needs, it necessarily becomes over exposed to the security risks faced by those companies.

Those risks could derive from dramatic external factors, like hacks targeted on a single major supplier, or from more mundane maintenance issues: if a number of Government Departments rely on a single large digital supplier for instance, there is a greater risk of widespread service disruption when that supplier needs to update security patches across all of its software simultaneously, or if corporate relations with the supplier simply turn sour.

Similarly, by encouraging a more diverse digital supplier network, the Government is more likely to benefit from new innovations as it tries to address tech challenges that have already made themselves known, as well as those we will encounter in the future. In other words, the chances of solving digital problems are improved if there are more companies working on those problems in the first place. This, in part, why the Government established the GDS advisory board and gave it an explicit mandate to "evaluate how emerging digital and technology trends can be applied to public services".

The Government had committed to establishing "a clear approach for protecting information across the whole of the public sector and delivery partners" by December 2017 and one would hope to see this commitment honoured after the general election in

> ***"94% of government procurement with digital & technology suppliers continues to be with large enterprises"***
>
> **National Audit Office**

June. Part of that solution can be found in developing a more diverse supplier base by commissioning a greater proportion of public sector contracts by value through and with SME suppliers.

Eroding the tax base?

Suppliers to Government are keen to ensure competition keeps a check on prices and drives up value for public sector customers. Over-reliance on a small number of foreign companies could make that harder – UKCloud worries that "there is a real risk that the government will become locked into a few global technology companies, and in doing so be at the mercy of currency fluctuations and other price rises". Domestically, greater use of UK-based SMEs in the digital supplier network could also help the Government stem the "erosion of the tax base" – an objective that has been clearly enunciated by both the Prime Minister and the Chancellor as we move towards an increasingly digital economy. In her Davos speech, Theresa May stressed the importance of "businesses paying their fair share of tax [and] genuinely investing in – and becoming part of – the communities and nations in which they operate".

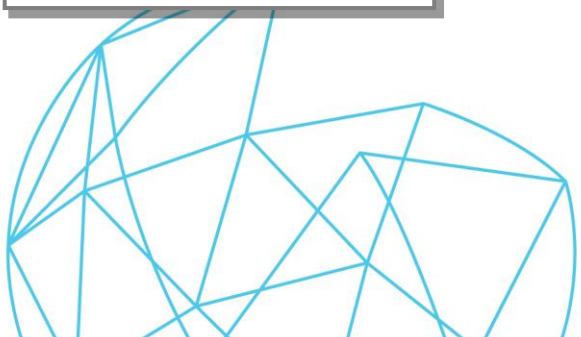
The Government has already started to examine how it can encourage large companies with headquarters in other tax jurisdictions to meet public expectations of their UK tax liabilities. In last year's Budget, for example, the Government stressed that "HMRC will be able to require non-compliant overseas traders to appoint a tax representative in the UK, and will be able to inform online marketplaces of the traders who have not complied". If the Government intends to protect the tax base in the digital retail sector, there are corresponding reasons for protecting the tax base through public sector digital procurement.

A clear commitment from the next Government to increase the value of digital contracts secured with and through SMEs would encourage more digital start-ups to launch in the UK in the first place, too. Again, this would make expansion of the digital tax base more likely – as more companies would be incorporating and paying their taxes within the UK.

This would be in line with existing policies designed to support growing tech clusters in the UK and a more benign regulatory environment for incubators (like the FCA's "regulatory sandbox") for start-ups in new digital industries.

"Evaluate how emerging digital and technology trends can be applied to public services"

GDS Advisory Board mandate



GUIDE
CLEAR THINKING

ukcloud

In association with UKCloud

There is now an opportunity for private sector suppliers to inform the next Government's approach to protecting data and boosting digital public sector procurement. DCMS has launched a "call for views" consultation on the EU's General Data Protection Regulation (GDPR will become law in the UK in May 2018) and suppliers are free to submit a response over the coming days.

More importantly, during the general election campaign there will be a chance for each political party to set out its proposals to protect sensitive Government data stored both inside and outside the UK, as well as their plans to encourage a more diverse digital supplier base. Clarity here would be welcomed by private sector suppliers and public sector users alike.

GUIDE
Spring 2017