



Access
Partnership

Public Procurement and Cloud Service Providers in the United Kingdom

4 JUNE 2018



Summary

The United Kingdom (UK) has systematically embraced electronic procurement methods and cloud-first as core policies to achieve cost savings, efficiency, and reliability for government agencies. The UK's central procurement procedures are solely handled through e-procurement platforms, including an exclusive digital marketplace which handles public sector procurement for digital goods and services, such as cloud.

The government's [cloud-first policy](#) has promoted cloud adoption across all government agencies, acting as a vote of confidence in broader cloud uptake across UK society, including in the financial and health sectors. Since then, the government's G-Cloud framework and progress toward becoming a "[cloud native](#)" has pushed the government towards adopting and seeking further innovation in cloud solutions in order to provide high-level, scalable, and reliable e-government services to its constituents. The UK also issues regular reports and cloud guidance regarding the implementation of data protection, security, and privacy recommendations across sectors.

As experts in the field of regulatory policy, Access Partnership has the knowledge and expertise to help guide clients through the cloud procurement landscape. Our public policy specialists have a thorough understanding of the regulatory environment across the UK, the EU, and its member states, and possess extensive sector-specific knowledge, particularly in the fields of finance and health. These attributes allow us to provide our clients with comprehensive solutions to help achieve their goals with minimal fuss.

This report examines the regulations, rules and procedures surrounding procurement, and more specifically cloud procurement, in the UK. We provide a snapshot of the laws, regulations, and guidance that may impact cloud uptake and outsourcing in public, financial, and healthcare sectors.

Overview of Cloud Computing in the UK

When the UK government adopted its G-Cloud computing strategy in 2010, 38% of public-sector organisations reported using cloud-based services. Today, the figure is 82%. G-Cloud is now moving towards its tenth iteration, predicted to launch in early 2019, which will invite new applications from suppliers.

Cloud computing allows the public sector — from health and education to the police and departments in the Treasury — to perform services in a cost-efficient, time-saving, and user-friendly manner. The strategy successfully transformed government information and communication technology, although organisations like the NHS still conduct the vast majority of their workload outside cloud software

Information-sharing of health, revenue, and police records provides greater transparency across public-sector organisations. Still, most government-owned data remains highly sensitive, thereby demanding coordination between organisations and cloud providers on security and privacy. With easy access comes greater security concerns: from ensuring proper identification to detecting and preventing attacks. Public-sector organisations therefore resort to a hybrid IT approach by combining in-house and cloud-based services.

The UK's rules for cloud procurement contrasts with the EU, which does not have set regulations. Instead, the European Commission funded the Procurement Innovation for Cloud Services in Europe project (PISCE) to develop tender-drafting guidance. However, the EU requires data processors to follow the EU General Data Protection Regulation (GDPR) — which 18 countries have yet to adopt, although the UK has transposed it into national law and will follow its provisions after Brexit.

Public Procurement Framework in the UK

The UK government is well ahead in cloud policy; [adopting a cloud-first policy five years ago](#) and now moving to “[cloud native](#).” The Government Digital Service (GDS), part of the Cabinet Office, is working with the Crown Commercial Service — in charge of the digital transformation of government— to develop new guidance. Their work on the digital procurement agenda will promote cloud, but work remains to be done to help staff fully understand and harness the benefits of cloud.

Crown Commercial Service and the Digital Marketplace

The Crown Commercial Service (CCS) provides commercial and procurement services to the public sector. CCS agreements cover a wide array of services, including communications, e-commerce, energy, technology, and office solutions, among others. They also maintain and operate several procurement platforms, including the core [eSourcing Portal](#) and [Digital Marketplace](#) platforms.

Potential CCS suppliers are required to register on the eSourcing Portal to participate in CCS tender opportunities. While registering for access to the eSourcing Portal does not instantly make a registrant a CCS supplier, it does allow and encourage a registrant to respond to tender opportunities.

For cloud technologies and specialist services for digital projects, public-sector organisations and agencies use the Digital Marketplace as the primary procurement platform. Cloud hosting, software, and support

can be found in the marketplace's G-Cloud framework, where cloud service suppliers (CSPs) must apply within a set application window to be accepted as a potential supplier.

G-Cloud Framework

The G-Cloud framework is a catalogue of services (infrastructure, platform, software, and cloud support) where basic terms of use have already been agreed upon between the government and suppliers. This allows buyers to acquire services without running a full Official Journal of the EU (OJEU) procurement process each time (each iteration of G-Cloud invites tenders for these suppliers through the OJEU process when it's launched.) Buyers are able to prepare their requirements, create a shortlist, and compare services to find the best value and award the contract online. Public sector organisations must follow the [Technology Code of Practice](#) which sets standards on the best way to design, build, and buy technology. Among the key principles is the government's [cloud-first policy](#), which requires procuring actors to seek and adopt cloud technologies first and foremost, aiming for fluid interoperability.

To sell services through the Digital Marketplace, a CSP will need to apply to the G-Cloud framework at the beginning of each iteration. The application requires information about the company's history, its service offering, operation strategy, service security, service costs, where cloud data will be stored, and whether their services are based on open standards. Once an applicant is accepted, it will have to pass a service and financial check. Although CSPs do not have to be based in the UK, they must agree to the terms of the framework agreement and contract governed by English law.

The application window for the existing G-Cloud framework, G-Cloud 9, is closed. The G-Cloud 10 framework will be accepting CSP applicants in early 2019.

Regulatory Landscape for Cloud in Financial Services

In 2016, the Financial Conduct Authority (FCA), the UK's financial sector regulator, released [guidance](#) on financial sector procurement of cloud computing services. The guidance aims to clarify requirements for financial firms when outsourcing to the cloud, as well as other third-party IT services, but is not binding. The guidance instructs financial firms to carry out a security risk assessment which includes the service provider and the technology assets administered by the firm. Concerning data protection, security, and data location issues, the guidance also refers financial firms to the [Data Protection Act \(DPA\) of 1998](#) and the Information Commissioner's Office (ICO) [guidance on cloud computing](#).

Regulatory Landscape for Cloud in the Healthcare Sector

On 19 January 2018, the National Health Services and Department of Health and Social Care released [guidance](#) on healthcare organisations using cloud services or data offshoring to store patient information. Part of the government's cloud-first policy, the NHS endorses the use and implementation of public cloud services to host NHS patient information.

Impact of the GDPR

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018 and extended the EU data protection regime to all foreign companies processing the data of EU residents. The harmonisation of data protection regulations throughout the EU should, in theory, make it easier for non-European businesses to comply with the regulations; however, it will require strict data protection compliance. As of June 2018, there are 18 countries who are yet to implement the GDPR in national legislation, while a lawsuit against Google and Facebook has already been filed for their supposed failure to adhere to the new regulations. In preparation for leaving the EU, the UK was one of the first to implement the GDPR in local law as part of the Data Protection Act 2018.

UK – Key Takeaways

- The UK's cloud-first policy was adopted five years ago and has seen considerable success in raising the proportion of public services using cloud services.
- CSPs hoping to bid on UK tenders must go through the G-Cloud process, in which a CSP must apply within a set time-window. Once accepted, CSPs may access tender opportunities through the [Digital Marketplace](#) platform.
- The application window for G-Cloud 9 closed in April 2017. The G-Cloud 10 framework will accept CSP applications in early 2019.
- The Financial Conduct Authority's (FCA) [guidance](#) clarifies requirements for financial firms seeking to outsource cloud services. The guidance refers financial services to consult the [Data Protection Act \(DPA\) of 1998](#) and the Information Commissioner's Office (ICO) [guidance on cloud computing](#) for issues relating to data protection, security, privacy and data location.
- The National Health Services and Department of Health & Social Care provides [guidance](#) on healthcare organisations who want to use cloud services or data offshoring to store patient information, referring healthcare providers to consult the DPA and GDPR for issues relating to data protection, security, privacy and data location.



Access Partnership

www.accesspartnership.com



[AccessAlerts](#)



[AccessPartnership](#)



9th Floor, Southside
105 Victoria Street
London SW1E 6QT

