Access Partnership

Public Procurement and Cloud Service Providers in Germany

Summary

Germany’s Digital Agenda 2014-2017 promoted digitalisation, internet use, technical skills, the buildout of e-government services, and movement towards broader cloud adoption — according to the federal government, successfully. In March 2016, the Federal Ministry of Economic Affairs and Energy released the new digital strategy, Digitale Strategie 2025, which notably implied that cloud can help meet goals.

In 2015, German IT officials agreed on terms for public sector cloud use under Resolution 2015/5 of the federal government’s IT Council. Under this resolution, Germany began developing the ‘Bundescloud,’ a cloud for federal government data hosting incorporating strict data protection and privacy schemes for government agencies.

The Resolution requires Bundescloud providers to sign a non-disclosure agreement promising to refrain from giving access to German data in foreign jurisdictions, such as the US, as well as requiring that sensitive information be stored on servers in Germany. Under these terms, the German government is only allowed to use cloud service providers (CSPs) certified by the government’s IT security office, the BSI, under the Cloud Computing Compliance Controls Catalogue (C5). In 2016, the BSI set C5 requirements as the mandatory minimum baseline for German government agencies to adopt public cloud solutions.

As experts in the field of regulatory policy, Access Partnership have 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 Germany, 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 Germany. 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 Public Procurement in Germany

Germany traditionally has a highly decentralised and complex procurement system due its federal system. About 58% of all procurement activity is done at the municipal level, 30% at the state level, and 12% at the federal level.

Germany has four central procurement bodies at the federal level: the Federal Financial Directorate Southwest (BFD Südwest) procures for the tax administration; the Federal Institute for Materials Research and Testing concludes framework agreements for specific technical product groups; the Federal Office for Equipment, IT Technology, and Use of the German Armed Forces is mainly responsible for procurement for the German military; and the Central Purchasing Body of the Ministry of the Interior procures for all federal agencies and manages the main e-procurement platform.

Germany, as with all EU member states, transposes the 2014 EU Procurement Directives into its national laws. Thus, central government authorities’ service contracts that exceed €144 000, and other, sub-central, public agencies’ service contracts exceeding €221 000 must publish public tenders through the Official Journal of the EU (OJEU) and its electronic online-platform, the Tenders Electronic Daily (TED). If service contracts do not exceed EU thresholds then tenders are to be placed through national procurement systems and procedures.

Germany follows the same procedural systems as the EU Directives mandate. Open procedure is Germany’s standard operating procurement procedure, followed by restricted, negotiated, and competitive procedures. Germany also favours framework agreements and joint procurement when tendering for services such as cloud computing.

A unique characteristic of the German procurement institutional set-up are Public Procurement Committees. These bodies bring together stakeholders from federal, state and local administrations, public-private organisations, and the private sector to help draft procurement rules, taking into account private and public sector needs. The German Committee for Supplies and Services Tendering and Contract Regulations (DVAL) works on procurement rules for supplies and services.

eProcurement

Since April 2017, EU central purchasing bodies are obliged to conduct procurement procedures above the EU thresholds in strictly digital form. Participation applications and offers are only accepted in digital form and the communication with the bidders should also be done in digital form. Germany switched to eProcurement methods in 2015, well ahead of the EU mandate.

Germany has placed all of its federal, state and municipal tenders on the centralised platform Bund.DE. For economic operators hoping to respond to an official tender, they must refer to the eVergabe platform. eVergabe provides a medium for companies to effectively communicate electronically with contracting authorities, as well as allowing contracting authorities to post tender opportunities. The platform provides a singular location where tender document submission, processing and tendering can be done, from enotification to e-award. The goal of the platform is to boost efficiency within the procurement framework for both sides of the arrangement, saving money and accelerating the tendering process.

As EU procurement directives stipulate, bidding companies must pass a certain level of scrutiny on their financial state, technical know-how, and potential past criminal activities. In Germany, companies that meet EU standards can seek prequalification for bidding on the eVergabe platform. Through pre-qualification, companies save time by reducing the number of submission requirements per tender, such as individual certificates (sales statements, trade and professional registration, and criminal background check) that are regularly required in procurement procedures. Once a bidder is prequalified, contracting authorities will recognise prequalification in place of individual certificates. By attaining prequalification, companies avoid award exclusions, such as incorrect submission of procurement documents, reduces document redundancy for tendering, and confirms the seriousness and efficiency of the company to contracting authorities.

Sustainable Procurement

Germany's public procurement system has been recognised an efficient instrument to attain Europe's 2020 Agenda objectives in respect to socio-economic goals, particularly SME procurement inclusion and sustainability requirements. Energy efficiency is a major issue in Germany's public procurement framework, expressly stated as a mandatory criterion for awards. Federal, regional and communal authorities work with the Alliance for Sustainable Procurement to increase sustainable government purchasing. CSPs can engage government stakeholders and demonstrate their offerings' potential energy savings as a point of contrast with less green legacy IT and physical infrastructure.

Regulatory Landscape for Cloud in Financial Services

Section 25b of the Banking Act, which applies to commercial banks and portfolio investors, regulates the outsourcing of functions essential for business operations and establishes baseline oversight requirements. Specifically, an outsourcing service must not impair:

- the proper execution of business or services;
- the ability or responsibility of managers from executing core management functions; or
- the functioning of the German Federal Supervisory Authority's (BaFin) right to request information, right to review, and ability to supervise.

"Suitable arrangements" — specifically a written contract stipulating rights and responsibilities — must be undertaken to ensure this. Other financial entities including securities traders and capital market institutions are regulated by the Securities Trading Act and the Investment Code, respectively, which contains similar requirements vis-a-vis outsourcing. Insurers are regulated by the Insurance Supervision Act, but also overseen by BaFin and subject to its rules.

The latest version of BaFin's Risk Management Circular (MaRisk 2017) was released in October 2017. It clarifies the definition of "outsourcing" to mean the provision of a service by an outside enterprise to provide activities or processes related to executing business, financial services, or other usual services that would otherwise have been performed by the financial institution itself. MaRisk requires that regulated institutions apply uniform policies group-wide addressing data management, data quality, and data aggregation risk. Data "structure and hierarchy" must be controlled so that it can be swiftly identified, merged, evaluated, and made available (Section AT 4.3.4). An independent Internal Audit function must also have "complete and unrestricted access" to information, whether or not it has been outsourced (Section AT 4.4.3). "Significant outsourcing" of core functions (this designation to be determined by the entity in question on the basis of a risk assessment) is permitted but brings a mandate that the contract address certain elements, including those to ensure adequate oversight and audit capabilities, and that data protection and safety requirements are respected (Section AT 9).

Provisions of the Banking Act and the Investment Act are further elaborated by a November 2017 BaFin circular on Regulatory Requirements for IT Systems (BAIT). This document interprets and provides clarification on existing obligations, including when processes are outsourced to a third-party. It addresses areas such as information risk management, information security management, and user authorisation management, including specially protected categories of information. In particular, BAIT interprets what is meant by "an appropriate technical and organisational configuration of IT systems," mandates a risk assessment before procurement of any external IT services and requires that regulated entities appoint an independent Information Security Officer that is responsible for overseeing and ensuring the security of third-party arrangements in accordance with the entities risk management strategy and assessments. It is expected that BAIT will serve as the template for similar rules for the insurance sector, currently under development, while BaFin and the German Federal Office for Information Security are still weighing the option to incorporate critical infrastructure rules into BAIT.

A recently published article by BaFin provides extended guidance on the regulatory framework for cloud computing in the financial sector. The article makes clear that supervised entities must refer to BAIT for general guidance on cloud computing. The article also clarifies that if a cloud service is considered material outsourcing, as laid out in section AT 9 of MaFin, then supervised entities must ensure they have unrestricted information rights and audit rights with their CSPs, as well as grant BaFin such unrestricted rights via the outsourcing contract between the supervised entity and the CSP. BaFin also plans to publish more detailed guidance on the issue of cloud computing over the course of 2018.

At the European level, in December 2017, the European Banking Authority (EBA) released a report providing guidance for financial services seeking to procure cloud services, giving a comprehensive set of considerations for financial sector entities to abide by when evaluating CSP offerings, including recommendations on contracting, right to physical access to business premises of CSPs, privacy issues, and security frameworks. The guidance works hand-in-hand with the 2006 CEBS guidance on outsourcing.

Regulatory Landscape for Cloud in the Healthcare Sector

Offering and using cloud solutions in the healthcare sector is governed by several sets of laws to ensure data protection. The Federal Data Protection Act (FDPA) and German Social Code regulate personal data protection and privacy, while the German Data Protection Authority's (DPA) cloud guidelines help align would-be cloud users and serve providers structure business arrangements. However, more recent reforms have been made. Due to the GDPR, the German Federal Assembly has approved a new Federal Data Protection Act, the German Data Protection Amendment Act (GDPPA), that adapts the FDPA to align with GDPR requirements.

Germany – Key Takeaways

- About 58% of all procurement activity is done at the municipal level, 30% at the state level, and 12% at the federal level.
- If procurement tenders are under the EU mandated thresholds, tenders are published through the Bund.DE platform. Bidding businesses can reply to tenders through the eVergabe platform.

  Under Resolution 2015/5, CSPs hoping to sell services to the federal government must sign a non-disclosure agreement promising to refrain from giving access to German data in foreign jurisdictions. CSPs are required to store sensitive government information on servers in Germany.
- The German government is only allowed to use CSPs certified by the government's IT security office, the BSI, under the Cloud Computing Compliance Controls Catalogue (C5). In 2016, BSI set C5 requirements as the mandatory minimum baseline for German government agencies to adopt public cloud solutions.
- Germany's procurement practices promote innovation, clean energy, and competitive inclusiveness.
- Germany has regulations in place for outsourcing essential business operations to third parties for financial services.
- The healthcare sector lacks concrete cloud guidance or regulations. However the Federal Data Protection Act (FDPA) and the German Data Protection Amendment Act (GDPPA) set out data protection rules for health-related data.

Access Partnership

www.accesspartnership.com

AccessAlerts

AccessPartnership

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