Regulatory Overview

Financial Services — Germany

AWS is committed to offering regulated entities (e.g., financial institutions or insurance companies) in Germany a strong compliance framework and advanced tools and security measures which they can use to evaluate, meet, and demonstrate compliance with applicable legal and regulatory requirements. This document provides AWS's regulated customers with information about the legal and regulatory requirements in Germany which may apply to their use of AWS services.

Financial institutions in Germany are **permitted** to use cloud services, provided that they comply with applicable legal and regulatory requirements, such as those described below.

Who is the regulator for financial institutions, insurance undertakings and similar institutions in Germany?

The Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht) ("BaFin") and the Deutsche Bundesbank ("Bundesbank") are Germany's financial supervisory authorities. BaFin supervises banks and other financial service providers, insurance undertakings and pension funds, stock exchanges, asset management companies and investment funds and securities and other investment companies. The Bundesbank undertakes the on-going supervisions of banks and financial service providers. Certain financial service providers (significant institutes) may be regulated by the European Central Bank.

What regulations apply to regulated entities in Germany using AWS?

Regulated entities in Germany may be subject to a number of different legal and regulatory requirements, when they use cloud services.

The German Banking Act (Kreditwesengesetz) ("KWG") applies to licensed banking and financial services institutions. The requirements on risk management set forth in KWG are further specified in two BaFin circulars: the Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement – "MaRisk") and the Banking Supervisory Requirements for IT (Bankaufsichtliche Anforderungen an die IT – "BAIT").

The German Act on Supervision Insurance Undertakings (Versicherungsaufsichtsgesetz) ("VAG") applies to insurance undertakings. The requirements for risk management are similar to the requirements for banking and financial services institutions and are also further specified in two BaFin circulars: the Minimum Requirements on Business Organisation of Insurance Companies (Mindesantforderungen an die Geschäftsorganisation von Versicherungsunternehmen, "MaGo") and the Insurance Undertaking Requirements for IT (Versicherungsaufsichtliche Anforderungen an die IT – "VAIT").

- The MaRisk or the MaGo respectively contains requirements regarding responsibility for risk management, insurance of continuity and quality of outsourced activities, cooperation with regulators and audit rights, data management, data security and confidentiality.
- The BAIT or the VAIT respectively, in part, further specifies the MaRisk or the MaGo respectively. It sets forth requirements on technical and organizational measures for IT systems, in particular regarding security and contingency plans.

There are other relevant EU and German laws and regulations in addition to MaRisk and BAIT, or MaGo and VAIT that pertain to regulated entities' use of cloud services (e.g., KAMARisk, KAIT, ZAIT). AWS encourages its regulated customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including the MaRisk, BAIT, MaGo, or VAIT and other local regulations, guidelines and laws.

Customers that have questions about the MaRisk and BAIT or MaGo and VAIT and how these may apply to their use of AWS services, or regarding any regulations, guidelines, and laws that might apply in this context, can reach out to their account representative.

Key considerations for regulated entities in Germany using AWS

AWS is committed to offering customers a strong compliance framework and advanced tools and security measures which customers can use to evaluate, meet, and demonstrate compliance with applicable legal and regulatory requirements.

Regulated entities who are using or planning to use AWS services can take the following steps to better understand their compliance needs:

1. Consider the purpose of the workload(s) under consideration and the relevant categories of data in order to anticipate which legal and regulatory requirements may apply.
2. Assess the materiality or criticality of the relevant workload(s) in light of local requirements. For example, see the materiality assessment considerations in Section AT 9.2 of the MaRisk or the risk assessment in accordance with item 247 of the MaGo.
3. Review the AWS **Shared Responsibility Model** and map AWS responsibilities and customer responsibilities according to each AWS service that will be used. Customers can also use **AWS Artifact** to access AWS's audit reports and conduct their assessment of the control responsibilities.
4. Customers that have further questions about how AWS services can enable their security and compliance needs, or that would like more information, can contact their account representative.

Key data privacy and protection considerations for regulated entities in Germany using AWS

Regulated entities in Germany using AWS services should also consider applicable privacy requirements, including the General Data Protection Regulation ("GDPR") and the **German Federal Data Protection Act**. If customers process or are planning to process the personal data of data subjects in the European Economic Area (EEA), which includes the EU, they should visit **AWS's General Data Protection Regulation (GDPR) Center**. More information on these requirements is included in the AWS whitepaper, **Navigating GDPR Compliance on AWS**.

Additional AWS Resources

- AWS Compliance Quick Reference Guide
- Navigating GDPR Compliance on AWS
- Using AWS in the Context of Common Privacy and Data Protection Considerations
- Implications of the Code of Conduct for Cloud Infrastructure Service Providers in Europe

AWS Compliance Programs

C5

CISPE

ISO 9001

ISO 27001

ISO 27017

ISO 27018

PCI DSS Level 1

SOC

ISAE 3000 Type 2

CSA