Regulatory Overview

Financial Services — Estonia

AWS is committed to offering financial institutions in Estonia 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 page provides AWS financial institution customers with information about the legal and regulatory requirements in Estonia which may apply to their use of AWS services.

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

Who is the Financial Regulator in Estonia?

Finantsinspektsioon (Financial Supervision Authority) is Estonia's financial supervisory authority and supervises, inter alia, credit institutions, securities markets and brokers, fund managers, payment services providers, investment firms, and insurance and reinsurance companies. The main objective of supervision is to ensure that financial institutions are able to meet their obligations to the customers in the future - pay out deposits, insurance losses or pension contributions, etc. and also to help increase the efficiency of the financial sector in Estonia, avoid systemic risks, and prevent the abuse of the financial sector for criminal purposes.

What regulations apply to financial institutions in Estonia using AWS?

Financial institutions in Estonia may be subject to a number of different legal and regulatory requirements when they use cloud services. For example, Finantsinspektsioon has confirmed the applicability of the **European Banking Authority Guidelines** on outsourcing arrangements issued 25 February 2019 ("EBA Guidelines") in Estonia. The EBA Guidelines apply to EU-regulated credit institutions, investment firms, electronic money institutions and payment institutions, and provide guidance to these entities when they are using or planning to use cloud services. This guidance covers a variety of contractual and operational areas, including audit rights, security of data and systems, location of data and data processing, sub-outsourcing, and contingency plans and exit strategies. Customers that have questions about the EBA Guidelines, and how these may apply to their use of AWS services, can reach out to their account representative or **contact us**.

Local regulations, guidelines, and laws in Estonia may also apply to financial institutions in Estonia when they use cloud services. This includes the **Advisory Guidelines of the Financial Supervision Authority on Outsourcing Requirements for Supervised Entities issued 25 October 2006** and the **Creditors and Credit Intermediaries Act**.

Regulations are changing rapidly in this space, and AWS is working to help customers proactively respond to new rules and guidelines. AWS encourages its financial institutions customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, including the EBA Guidelines and local regulations, guidelines, and laws.

Key considerations for financial institutions in Estonia 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.

Financial institutions 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, Section 4 of the **EBA Guidelines** contains materiality assessment considerations for financial institutions.
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' 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 or **contact us**.

If you have questions about using AWS services or need more information, please **contact us**.

Key data privacy and protection considerations for financial institutions in Estonia using AWS

Financial institutions in Estonia using AWS services should also consider applicable privacy requirements, including the General Data Protection Regulation ("GDPR") and the **Personal Data Protection Act (PDPA)**. If customers process or are planning to process the personal data of data subjects in the European Union (EU), they should visit **AWS' General Data Protection Regulation (GDPR) Center**. More information on these requirements are included in the AWS whitepaper, **Navigating GDPR Compliance on AWS**.

Additional AWS Resources

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

AWS Compliance Programs

CSA

GDPR

ISO 9001

ISO 27001

ISO 27017

ISO 27018

PCI DSS Level 1

SOC