Data protection and security for financial services

Key things you need to know

Financial services institutions are moving to the cloud. In turn, regulators are scrutinizing firms' ability to adapt to and recover from operational disruptions, particularly when it comes to data.

The key regulatory developments of concern include those around data privacy and cyber security, plus GDPR and Schrems II for those conducting business both in and with European financial institutions.

Data privacy

Financial services firms are being asked by regulators to identify critical information assets, and the infrastructure upon which they depend. Cyber security efforts should also be prioritized based on the significance of these information assets to the bank's critical operations.

Remote access, rapid deployment and bandwidth expansion considerations:

Risk mitigation: Pre-emptively calculate potential risks associated with a disruption or compromise to technology and/or applications.

Management: Define, document and roll out processes that include remote asset use, privileged users and application development.

ICT partnership: Update ICT teams regularly, including cyber security to maintain the correct posture to accommodate long-term remote access.

It's imperative that you develop plans to maintain critical information integrity following a cyber event and regularly evaluate the threat profile of critical information assets. It's also important to regularly test for vulnerabilities and ensure resilience against ICT-related risks.

Cyber security

Not only have cyberattacks become increasingly sophisticated, they now have a greater potential to disrupt individual institutions as well as entire markets due to greater digitalization, interconnectedness, and reliance on third parties.

Maintaining and improving enterprise resilience is a new way for an organization to build trust with customers and regulators.

European Central Bank levels of expectation for financial market infrastructures:

Evolving: Essential capabilities established, evolved, and sustained to identify, manage and mitigate cyber risks. Performance of practices monitored and managed.

Advancing: In addition to previous level, implement more advanced tools, integrated across business lines and improved over time to proactively manage cyber risks.

Innovating: In addition to previous levels, drive innovation in people, processes, and technology for the FMI and the wider ecosystem to manage cyber risks and enhance cyber resilience. This may require new controls and tools development or new information-sharing group creation.

Technology assets should be kept up to date and patched to mitigate against new and existing cyber threats and out-of-support technology. Major change programs may need to be established to tackle any technology debt.

teradata.

Schrems II

This ruling is primarily about data sovereignty and controlling where PII is held/sits. With regards the transfer of personal data to the US, an adequacy arrangement was in place that recognized the US' Privacy Shield framework. This judgement, made in July 2020 by the European Court of Justice, effectively removes adequacy status for the Privacy Shield and brings uncertainty to data transfers between the US and EU.

The European Data Protection Board sets six steps for evaluating cross-border transfers and the importers' third countries:

- Exporters, know your transfers
- Verify the transfer tool your transfer relies on
- Assess if any law or practice in the third country may impinge on safeguard effectiveness for your transfer
- Identify and adopt measures to bring data protection levels up to the EU standard of essential equivalence for the data transfer
- Take any formal procedural steps for the adoption of these supplementary measures
- Re-evaluate at appropriate intervals and monitor any developments that may affect your data transfer

While Schrems II may not appear to impact the UK directly, as it sits outside the EU, the UK tends to "gold plate" regulation from the EU. They may not want to diverge from EU rulings or be seen to diverge from EU practices.

GDPR

This EU personal data law affects businesses worldwide and came into effect in 2018. GDPR advises what companies can and can't do with personally identifiable information (PII).

PII includes (but is not limited to):

Name	Social media use
Phone number	Geotags
Address	Health records
Date of birth	Race
Bank account	Religious beliefs
Passport number	Political affiliation

Any incident that leads to personal data being lost, stolen, destroyed, or changed is considered a data breach, and could lead to a fine of up to €20 million ($23 million) or 4% of annual global turnover.

What action should you take?

Data protection and security are major concerns for global financial services institutions of the future, as digital first will be the standard operating model. Flexibility will be an important factor for future success, so that any new regulation that impacts data handling can be met with minimal disruption. A new hybrid and multi-cloud infrastructure will bring the ultimate flexibility. It will grant the ability to shift data and move workloads between multiple cloud providers, and even back on-premises if necessary. And any data move will be swift – with minimal disruption.

About Teradata

Teradata is the connected multi-cloud data platform company. Our enterprise analytics solve business challenges from start to scale. Only Teradata gives you the flexibility to handle the massive and mixed data workloads of the future, today. The Teradata Vantage architecture is cloud native, delivered as-a-service, and built on an open ecosystem. These design features make Vantage the ideal platform to optimize price performance in a multi-cloud environment. Learn more at **Teradata.com.**

17095 Via Del Campo, San Diego, CA 92127 Teradata.com

teradata.