



DORA Statement

The Digital Operational Resilience Act, or DORA, is a European Union (EU) regulation that sets out a binding, comprehensive information and communication technology (ICT) risk management framework for the EU financial sector.

DORA establishes technical standards that financial entities and their critical third-party technology service providers must implement in their ICT systems by 17 January 2025. You can read more about DORA here <https://www.digital-operational-resilience-act.com/>

Informatica recognized the need for ICT providers to be proactive and provide (optional) contract enhancements to allow its financial services customers to comply with DORA. We updated our Financial Services Addendum optimized for DORA with the five pillars in mind:



1. ICT Risk Management :
ICT providers must ensure robust systems to detect and mitigate risks (e.g., cybersecurity attacks, system failures).



2. Incident Reporting:
Financial entities must report significant incidents (cyberattacks, service disruptions) to relevant authorities within tight deadlines.



3. Digital Operational Resilience Testing:
ICT Providers and Financial entities must undergo regular digital operational resilience testing.



4. Management of Third-Party Risk:
Establishment of frameworks for managing third-party risk.
Financial entities are held accountable for risks introduced by ICT service providers.



5. Information Sharing:
Encourages sharing threat intelligence among financial entities

Please contact the following addresses to discuss DORA or obtain a copy of the Informatica DORA Addendum

North America – dlegalus@informatica.com

Europe, Middle East, Africa and Latin America - dlegalemeala@informatica.com

Asia Pacific and Japan - dlegalapj@informatica.com