MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

04 January 2023

Regulation (EU) 2022/2554 and Amending Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector published on the EU Official Journal

This circular is an update to circular titled Provisional Agreement Reached on the Digital Operational Resilience Act (DORA) published by the Authority in July 2022. Following the process of interinstitutional negotiations at a European Union (EU) level, the Regulation and accompanying Amending Directive were subject to voting in the European Parliament and the Council. The text was officially adopted in November 2022.

On 27 December 2022 Regulation (EU) 2022/2554 and Amending Directive (EU) 2022/2556 were published on the Official Journal of the EU and will enter into force on 16 January 2023. The Regulation, which amends Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, will apply from **17 January 2025**. The Amending Directive amends Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 and Member States are to adopt the measures necessary to comply with it also by **17 January 2025**.

Work on the Regulation continues as it will be supplemented by a series of Regulatory/Implementing Technical Standards, Guidelines, Reports, Recommendations and Calls for Advice. These will have different delivery deadlines as detailed in Annex 1.

DORA introduces provisions, subject to different layers of proportionality, on financial entities in the areas of ICT risk management, ICT-related incident management, classification and reporting, digital operational resilience testing (including advanced testing based on TLPT), managing of ICT third-party risk (including an Oversight Framework of critical ICT-third party providers) and voluntary information-sharing arrangements.

Overall, DORA is a complex cross-sectoral Regulation which introduces a series of novel, directly applicable, requirements. It is recommended that Authorised Persons start with the necessary preparations to ensure compliance with the Regulation.

On 27 December 2022, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) and Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive) have also been published on the EU Official Journal. The Authority will provide further information on these Directives accordingly.

Authorised Persons may request further information by sending an email to the Supervisory ICT Risk and Cybersecurity function within the MFSA on sirc@mfsa.mt.

Annex 1 – DORA Policy Work and Deadlines

	Jan-24	Jul-24	Jan-25
1. Guidelines on the estimation of aggregated annual cost/losses caused by major ICT-related incidents (Art. 11.10)		●	
2. RTS on ICT risk management framework (Art. 15)	●		
3. RTS on simplified ICT risk management framework (Art. 16)	●		
4. RTS on criteria for the classification of ICT-related incidents (Art. 18.3)	●		
5. RTS on specifying the reporting of major ICT-related incidents (Art. 20.1a)		●	
6. ITS to establish the reporting details for major ICT-related incidents (Art. 20.1b)		●	
7. Feasibility report for establishing a single EU Hub for major ICT-related events (Art. 21)			●
8. RTS to specify threat led penetration testing aspects (Art. 26)		●	
9. RTS to specify the policy on ICT services (Art. 28.2)	●		
10. ITS to establish the templates for the Registrar of Information (Art. 28.3)	●		
11. RTS to specify elements when sub-contracting critical or important functions (Art. 30.2a)		●	
12. Guidelines on cooperation between ESAs and CAs regarding the structure of the oversight (Art. 32.7)		●	
13. RTS to specify information on oversight conduct (Art. 41)		●	