MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

13 October 2022

Reporting of Major ICT-Related Incidents

Following a public consultation process published on 12 July 2022, the Malta Financial Services Authority ('MFSA', 'the Authority') is releasing the following material, available on the MFSA website (*Our Work > Supervisory ICT Risk and Cybersecurity*):

1. A Major ICT-Related Incident Reporting Process ('the Process Document');
2. Templates for Initial, Intermediate and Final Major ICT-Related Incident Reporting ('the Templates', 'the provided Templates');
3. User Guidelines for submitting Major ICT-Related Incident Reports to the Authority ('the User Guidelines').

A Feedback Statement document is also being issued alongside this Circular with the conclusions of the public consultation process.

The Authority expects all eligible Authorised Persons (see *Annex A – Exceptions*) to report Major ICT-Related Incidents, whether of an operational or security nature, to the Authority, in line with the Process Document, using the provided Templates, and by following the User Guidelines.

Major ICT-Related Incident reporting will eventually have to be aligned with the Digital Operational Resilience Act (at the time of writing, further information regarding this Regulation is provided in Circular titled Provisional Agreement Reached on the Digital Operational Resilience Act [DORA]).

Authorised Persons that have, in the past few weeks, notified an ICT-Related Incident that meets the thresholds, and therefore classifies as 'Major', are not expected to report the incident to the Authority again using the new process unless otherwise requested specifically by the Authority.

The content of this Circular and the above material **apply from the date of publication of this Circular** (13 October 2022), and supersede Circular titled Cybersecurity – Threat Mitigation issued on 25 September 2019.

This Circular does not replace or supersede any legal obligation by Authorised Persons to report incidents to other competent authorities, inter alia:

- the competent authority under Directive (EU) 2016/1148 (NIS Directive), transposed into Legal Notice 216 of 2018 of the Laws of Malta;
- the competent authority under Regulation (EU) 2016/679 (GDPR).

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

Annex A - Exceptions

Credit and financial institutions (payment institutions, electronic money institutions and account information service providers) are currently required to follow the EBA Revised Guidelines (EBA/GL/2021/03) on Major Incident Reporting under Directive (EU) 2015/2366 (PSD2) and to report major incidents using the reporting templates and methodologies stipulated within these Guidelines to the Central Bank of Malta under the Banking Act (Chapter 371 of the Laws of Malta) and the Financial Institutions Act (Chapter 376 of the Laws of Malta). Significant credit institutions are required to – in addition – report significant cyber incidents to the European Central Bank (ECB) via their allocated Joint Supervisory Team, using an agreed process and template established by the ECB. In view of this, the Process Document will not apply to credit and financial institutions.