MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

17 January 2025

Cyber Reporting Management System (CRMS)

This Circular is an update to Circular titled Regulation (EU) 20222554 and Amending Directive (EU) 20222556 on Digital Operational Resilience for the Financial Sector published on the EU Official Journal published by the Authority in January 2023 and to Circular titled Necessary Legal Measures Published for the Purposes of the National Implementation of Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector published by the Authority on 11 November 2024.

Once Regulation (EU) 2022/2554 (the 'DORA Regulation') becomes applicable, that is, as of 17 January 2025, pursuant to Chapters III *ICT-related incident management, classification and reporting* and Chapter VI *Information-sharing arrangements*, Authorised Persons within scope of the DORA Regulation (see Article 2 of the DORA Regulation); 1) shall report Major-ICT-Related Incidents, 2) are to notify Significant Cyber Threats on a voluntary basis, and 3) shall notify their voluntary participation in, or, as applicable, the cessation of their membership from, Information-Sharing Arrangements to the Authority.

Authorised Persons shall fulfil these obligations through the Cyber Reporting Management System (CRMS) within the License Holder (LH) Portal, using the provided Templates as explained further below.

Major ICT-Related Incidents

On 27 December 2022, the DORA Regulation and Directive (EU) 2022/2556 (the 'DORA Amending Directive') were published on the Official Journal of the EU and entered into force on 16 January 2023, introducing changes to incident reporting obligations. The obligation for the entities referenced under Article 2(1), point (a) to (d) of the DORA Regulation – being credit institutions, payment institutions (including those exempted under Directive (EU) 2015/2366), account information service providers, and electronic money institutions (including those exempted under Directive 2009/110/EC) – to report incidents under Directive (EU) 2015/2366 ('PSD2') will no longer apply and will be replaced by new reporting obligations under the DORA Regulation, by virtue of the DORA Amending Directive.

This change aligns with Recital 23 of the DORA Regulation, which aims to reduce administrative burdens and eliminate duplicative reporting obligations by establishing a single harmonised incident reporting mechanism for all operational or security payment-

related incidents, regardless of whether they are ICT-related. The ICT security controls and reporting requirements under PSD2 will be amended to align with the DORA Regulation, as highlighted in Recital 7 and Article 7(2)(ii)(f) of the DORA Amending Directive.

This Circular supersedes Circular titled Reporting of Major ICT-Related Incidents. All Authorised Persons in scope of the DORA Regulation (see article 2 of the DORA Regulation) have an obligation to classify Major-ICT Related Incidents as specified in Chapter II of Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024, supplementing the DORA Regulation with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents and report them in line with the stipulated timeframes defined in Article 5(1) of Commission Delegated Regulation (EU) ../.. of ../.., supplementing the DORA Regulation with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats (note that the RTS is not yet in its final version and is subject to change).

The Authority is releasing the following material, available on the MFSA website (under *Our Work > Supervisory ICT Risk and Cybersecurity*):

1. Major-ICT Related Incidents Reporting Process;
2. Template for Major ICT-Related Incident Reports;
3. User Guidelines for submitting Major ICT-Related Incident Reports to the Authority.

The above also applies to all other Authorised Persons not in scope of the DORA Regulation on an expectation basis, from the date of publication of this Circular, that is, 17 January 2025.

Significant Cyber Threats

All Authorised Persons within the scope of the DORA Regulation are to notify Significant Cyber Threats, to be determined in accordance with Chapter III, Article 10 of Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024, supplementing the DORA Regulation with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents, to the Authority on a voluntary basis.

The Authority is releasing the following material, available on the MFSA website (under *Our Work > Supervisory ICT Risk and Cybersecurity*):

1. Significant Cyber Threat Notification Process;
2. Template for Significant Cyber Threat Notifications;
3. User Guidelines for submitting Significant Cyber Threat Notifications to the Authority.

The above also applies to all other Authorised Persons not in scope of the DORA Regulation on a voluntary basis, from the date of publication of this Circular, that is, 17 January 2025.

Information-Sharing Arrangements

As an update to Circular titled Information Sharing Arrangements under Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, Authorised Persons within scope of the DORA Regulation (see Article 2 of the DORA Regulation) have an obligation to notify the Authority of their voluntary participation in, or cessation of membership from, an Information-Sharing Arrangement.

The Authority is releasing the following updated material, available on the MFSA website (under *Our Work > Supervisory ICT Risk and Cybersecurity*):

1. Information-Sharing Arrangement Notification Process;
2. Template for Information-Sharing Arrangement Notifications;
3. User Guidelines for submitting Information-Sharing Arrangement Notifications to the Authority.

The above continues to apply to all other Authorised Persons not in scope of the DORA Regulation on a voluntary basis.

The Malta Financial Services Authority expects all Authorised Persons to ensure that they have the necessary access to the CRMS Project within the LH Portal.

The above three processes do not replace or supersede any legal obligation by Authorised Persons unless that legal obligation is specifically superseded by the DORA Regulation.

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