MFSA MALTA FINANCIAL SERVICES AUTHORITY

Consultation Document

Consultation Document on the Reporting of Major ICT-Related Incidents

Ref: 05-2022

Date: 12 July 2022

Closing Date: 5 August 2022

NOTE: The documents circulated by the MFSA for the purpose of consultation are in draft form and consist of proposals. Accordingly, these proposals are not binding and are subject to changes and revisions following representations received from licence-holders and other involved parties. It is important that persons involved in the consultation bear these considerations in mind.

Contents

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155

communications@mfsa.mt
www.mfsa.mt

Introduction

"*The lack of consistent information on the nature and consequences of ICT-related incidents impedes the proper calibration and implementation of prudential requirements and the development of suitable policy responses*"[1].

In line with paragraph 4.8.11 of the Guidance Document, and in view of the outstanding times of heightened cyber threats, and in preparation for the entry into force of the Digital Operational Resilience Act (DORA), the Malta Financial Services Authority (Authority) is establishing an updated major ICT-related incident reporting process superseding the process communicated on 25 September 2019 titled Cybersecurity – Threat Mitigation.

In establishing the updated process, the Authority takes into consideration the challenges with the current incident reporting process (an Authorised Person may not have all the incident details in place at the time of initial reporting, for instance), the course that DORA is expected to be taking, and established incident reporting guidelines[2]. This process will eventually have to be aligned with DORA when it enters into force.

The Process

The Authority will expect the reporting of ICT-related incidents, whether of an operational or security nature, that reach the specified thresholds in Annex 1 – and therefor classify as 'major'. This will apply to all eligible Authorised Persons (see *Exceptions* section) in a three-tier approach: an *Initial Report*; an *Intermediate Report*; and a *Final Report* (see the draft Major ICT-Related Incident Reporting template published alongside this consultation document).

Authorised Persons will be expected to submit:

1. An *Initial Report* within **four (4) hours** after an incident has been classified as major. Such classification is expected to take place within **twenty-four (24) hours** after an incident has been detected.

2. An *Intermediate Report* within **three (3) working days** from the submission of the *Initial Report*, irrespective of whether the incident has been resolved. An Authorised Person may provide one or more *Intermediate Report/s* at different stages within the resolution process.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0198
[2] EBA Revised Guidelines on major incidents reporting under PSD2 (EBA/GL/2021/03)

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

3. A *Final Report* within **twenty (20) working days** after business is deemed back to normal.

This updated process 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).

The Authority will communicate the method to securely submit Major ICT Related Incident Reports at a later stage.

Exceptions

Credit and financial institutions 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 forms 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 being proposed within this document will not apply to credit and financial institutions.

Consultation Period

Any comments or feedback in relation to the updated process are to be addressed to the Supervisory ICT Risk and Cybersecurity function within MFSA by sending an email to mirt@mfsa.mt, referring to this Consultation, by not later than **Friday 5 August 2022**.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Annex 1 – Major Incident Thresholds Matrix

Authorised Persons are to classify as major those operational or security incidents that fulfil:

- one or more criteria at the higher impact level (third column); or
- three or more criteria at the lower impact level (second column).

CRITERIA	THRESHOLD FOR LOWER IMPACT LEVEL	THRESHOLD FOR HIGHER IMPACT LEVEL
TRANSACTIONS AFFECTED (WHERE APPLICABLE	More than (>) **10%** of the regular level/number of transactions **AND** a duration of the incident of more (>) than **one (1) hour** **OR** A total value of more than (>) **€500,000 AND** a duration of the incident of more (>) than **one (1) hour**	More than (>) **25%** of the regular level/number of transactions **OR** A total value of more than (>) **€15,000,000**
USERS AFFECTED	More than (>) **10% AND** a duration of the incident of more (>) than **one (1) hour** **OR** More than (>) **5,000 AND** a duration of the incident of more (>) than **one (1) hour**	More than (>) **25%** **OR** More than (>) **50,000**
SERVICE DOWNTIME	More than (>) **Two (2) hours**	Not applicable
BREACH OF SECURITY OF NETWORK OR INFORMATION SYSTEMS	Not applicable	Whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) of the Authorised Person
ECONOMIC IMPACT	Not applicable	More than (>) the maximum of (**0.1% Tier-1 Capital €200,000**)

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

		OR More than (>) **€5,000,000**
HIGH LEVEL OF INTERNAL ESCALATION	Yes	Yes, and a crisis mode (or equivalent) is likely to be triggered
GEOGRAPHICAL SPREAD	Up to **two (2) Member States**	More than (>) **two (2) Member States**
OTHER AUTHORISED PERSONS OR RELEVANT INFRASTRUCTURES POTENTIALLY AFFECTED	Yes	Not applicable
REPUTATIONAL IMPACT	Yes	Not applicable

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt