MFSA MALTA FINANCIAL SERVICES AUTHORITY

Feedback Statement

Feedback Statement on the National Implementation of Regulation (EU) 2022/2556 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector

Ref: L-0001-2024

Date: 27 March 2024

Contents

1. Introduction

On 16 January 2024, the Malta Financial Services Authority (the 'Authority' or the 'MFSA') released a Consultation Document on the National Implementation of Regulation (EU) 2022/2554 and Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector (the 'Public Consultation'). The purpose of the Public Consultation was to gather the views of Authorised Persons and other interested stakeholders on the proposed legal measures required for the implementation of Regulation (EU) 2022/2554 (the 'DORA Regulation') and the transposition of Directive (EU) 2022/2556 (the 'DORA Amending Directive').

The Authority would like to thank Authorised Persons and interested stakeholders for the feedback provided throughout the month-long consultation period.

This Feedback Statement is structured as follows:

- **Section 2 '*General Requests for Clarification and Guidance*':** Stakeholders raised an element of general queries asking for guidance on selected issues pertaining to the DORA Regulation, not necessarily related to the proposed legal measures. These general queries do not constitute direct feedback on the Public Consultation and have been answered in this section.

- **Section 3 '*Requests for Clarification and Guidance in Relation to the Proposed Legal Measures*':** The Authority received a number of requests for clarification related to the proposed legal measures that do not constitute direct feedback to the Public Consultation. These requests for clarification have been answered in this section.

- **Section 4 '*Feedback Received in Relation to the Proposed Legal Measures*':** The Authority received feedback directly related to the proposed legal measures. This section provides the feedback received in this regard and the respective Authority's position together with the rationale.

Lastly, the Authority invites stakeholders to read this Feedback Statement in conjunction with the Feedback Statement to Queries Raised by Consulted Stakeholders on Regulation (EU) 2022/2554 on Digital Operational Resilience (the 'DORA Regulation'), which has already clarified a number of queries raised by stakeholders during this Public Consultation.

2. General Requests for Clarification and Guidance

Requests Previously Clarified by the Feedback Statement to Queries Raised by Consulted Stakeholders

Feedback Received

Stakeholders raised an element of general queries asking for guidance on selected issues pertaining to the DORA Regulation, not necessarily related to the proposed legal measures, more specifically:

1. Stakeholders requested the Authority to provide more details on its planned approach to determine the scope, frequency, and execution of Threat-Led Penetration Testing ('TLPT') exercises for financial entities within scope;

2. Stakeholders asked for clarification on what is expected to be included in Financial Entities' Digital Operational Resilience Strategy;

3. Stakeholders asked for guidance on how to identify Financial Entities' critical or important functions.

Authority's Reply

The Authority notes that queries 1 to 3 above had already been previously raised and duly replied to by the Authority via the Feedback Statement to Queries Raised by Consulted Stakeholders on Regulation (EU) 2022/2554 on Digital Operational Resilience (the 'DORA Regulation'), published by the Authority in February 2024. Stakeholders are kindly invited to refer to the above-mentioned Feedback Statement.

Guidance on the Definition of Major ICT-Related Incidents

Feedback Received

Stakeholders asked for a clarification on what could consist a Major ICT-Related Incident under the DORA Regulation, including whether non-receipt of data from partners could be considered as a Major ICT-Related Incident.

Authority's Reply

In relation this query, it should be noted that Article 3(10) of the DORA Regulation defines a Major-ICT Related Incident as:

> "*an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity.*"

Chapter III of the DORA Regulation on Incident Management, Classification and Reporting is to be supplemented by three technical standards. One such technical standard is set to specify the criteria, including materiality thresholds for determining Major ICT-Related Incidents. Interested stakeholders are invited to refer to the Final Report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554, released by the European Supervisory Authorities (the 'ESAs').

The Authority's Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements

Feedback Received

Stakeholders asked for a clarification on the scope and applicability of the Authority's Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements (the 'Guidance Document'), in light of the DORA Regulation.

Authority's Reply

The Authority has provided a clarification in this regard via Circular titled Update on the Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements, as published by the Authority in March 2024. Interested stakeholders are kindly invited to refer to this Circular.

Interplay Between the DORA Regulation, ICT Third-Party Service Providers ('ICT TPPs') and Directive 2014/59/EU

Feedback Received

Stakeholders asked for a clarification on the interplay between the criticality assessment under Directive 2014/59/EU ('Bank Recovery and Resolution Directive' or 'BRRD') and the criticality assessment of an ICT Third Party Service Provider ('ICT TPP') in terms of the DORA Regulation. The specific areas of clarification are the following:

1. Should an ICT TPP be first assessed in terms of their criticality under the DORA Regulation or under the BRRD?

2. If an ICT TPP provides services that support critical or important functions under the DORA Regulation would this ICT TPP also be considered as critical for resolution planning in terms of the BRRD?

3. Does the Authority envision scenarios in which an ICT TPP identified as critical under the DORA Regulation is not considered as critical from a resolution planning perspective in terms of the BRRD?

Authority's Reply

The Authority would like to firstly clarify that there is a difference between an ICT TPP providing services that support critical or important functions to a financial entity and a Critical ICT TPP ('CTPP'), as designated in accordance with Chapter V Section II of the DORA Regulation.

An ICT TPP is an undertaking providing ICT services as defined by Article 3 (19), and the respondent needs to be further guided by Article 3 (22), which provides a definition of a critical or important function, for the identification of the ICT TPP/s supporting its critical or important functions. The Authority would also like to further draw the respondent's attention in relation to recital (70) of the DORA Regulation, reproduced below:

> *"The definition of 'critical or important function' provided for in this Regulation encompasses the 'critical functions' as defined in Article 2(1), point (35), of Directive 2014/59/EU.* ***Accordingly, functions deemed to be critical pursuant to Directive 2014/59/EU [BRRD] are included in the definition of critical functions within the meaning of this Regulation****."*

An ICT TPP providing ICT services that support a critical or important function does not have the same meaning as a CTPP, under the DORA Regulation. A CTPP is an ICT TPP identified as critical at a Union level. Those ICT TPPs designated as CTPPs will be subject to a Union-level Oversight Framework, as established by Chapter V Section II of the DORA Regulation. The identification of an ICT TPP supporting a critical or important function at a financial entity level is therefore different from the designation of a CTPP at a Union-level.

Notwithstanding the above, in relation to ICT TPPs providing ICT services that support a critical or important function to a Credit Institution, the Authority understands that the critically assessment should be approached in the following manner:

1. Credit Institutions should first assess whether they exercise any critical function in terms of the BRRD, which assessment is then confirmed or otherwise by the Resolution Committee;

2. Once a critical function is determined, Credit Institutions should then identify all relevant services, operational assets and roles/staff which are necessary for the continuity of the critical function(s) for the effective implementation of the resolution strategy in accordance with the Single Resolution Board's ('SRB') Operational Guidance on Operational Continuity in Resolution (OCIR). In carrying out such an assessment, ICT TPPs are likely to be captured as third parties providing critical services, amongst other non-ICT TPPs providing critical services.

3. Such services will then form part of a comprehensive list of services which are required to continue being offered by the Credit Institution post-resolution.

Therefore, the assessment under the SRB OCIR Guidance encompasses all types of critical service providers and is not limited to ICT TPPs under the DORA Regulation. In this regard, the criticality assessment under the OCIR Guidance and under the DORA Regulation are mutually exclusive.

Having said the above, the Authority recognises interlinkages between the two frameworks, and it is likely that an ICT TPP that provides ICT services that support a critical or important function under the DORA Regulation, would also be classified as a "critical service" under the SRB OCIR Guidance.

3. Requests for Clarification and Guidance in Relation to the Proposed Legal Measures

Criminal Offenses

Feedback Received

Stakeholders would like clarification on what is the legal basis for the laying down of criminal penalties, in accordance with the DORA Regulation. In addition, stakeholders have questioned what breaches of the DORA Regulation would constitute a criminal offence.

Authority's Reply

Member States may choose to lay down criminal penalties for breaches of the DORA Regulation pursuant to Article 52 of that Regulation. The DORA Regulation does not specify a list of breaches, and as a result neither does the draft *Digital Operational Resilience Act (DORA) Regulations, 2023.* Stakeholders are invited to refer to regulation 11 of the draft *Digital Operational Resilience Act (DORA) Regulations, 2023* for more details on criminal offenses.

Administrative Penalties and Other Administrative Measures in the Context of Major ICT-Related Incidents

Feedback Received

Stakeholders have asked for clarify on whether, in the case of a Major ICT-Related Incident, the same incident could incur different administrative penalties and other administrative measures across different regulations.

Authority's Reply

Each law stipulates obligations that shall be complied with by those persons to whom the respective legal provision/s is/are applicable. If an obligation is applicable to a particular person under two different laws, where such obligation is breached it would be punishable under each of those laws separately, in accordance with the applicable provisions of the laws in question.

4. Feedback Received in Relation to the Proposed Legal Measures

Centralisation of Incident Reporting

Feedback Received

Stakeholders have expressed positive views regarding the centralisation of incident reporting at a national level, in the context of the interplay between the DORA Regulation and Directives (EU) 2015/2366 and (EU) 2022/2555.

Authority's Position

The Authority takes note and positively welcomes the above-mentioned feedback.

Relationship Between Incident under the DORA Regulation and Reporting under Regulation (EU) 2016/679

Feedback Received

Stakeholders have presented concerns in relation to the fact that Financial Entities will be expected to report Major ICT-related Incidents to the Authority pursuant to the DORA Regulation, in addition to having to report incidents to the Information and Data Protection Commissioner ('IDPC') pursuant to Regulation (EU) 2016/679 (the 'General Data Protection Regulation', or 'GDPR').

Authority's Position

Stakeholders are to note that the scope of incident reporting under the DORA Regulation and that of the GDPR are different. Under the GDPR, financial entities have to report incidents which have had an effect on personal data only; whereas the incident reporting mechanism under the DORA Regulation has a broader scope. The ESAs have clarified this point via the Final Report on the Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554 [partially reproduced below]:

> *"In addition, the ESAs would like to clarify that DORA introduces requirements for digital operational resilience, which is different, in scope and objectives to GDPR. GDPR focuses on personal data while DORA has a larger scope. When it comes to the assessment of confidentiality, in accordance with Article 5 and*

13 of the draft RTS [Regulatory Technical Standard], it is for the FE [Financial Entity] to evaluate the level of confidentiality of the data." (p.68)

It is also relevant to add that the European Data Protection Supervisor ('EDPS') issued an opinion in relation to, *inter alia*, incident reporting under the DORA Regulation and under GDPR (see Opinion of the European Data Protection Supervisor on the Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014). In this opinion, the EDPS highlighted that there is a direct obligation on the data controller to report a data breach in accordance with Article 33 of GDPR and that direct reporting of a data breach to financial supervisors would be incompatible with the GDPR.

In addition to the above, for avoidance of doubt, it should be noted that the incident reporting mechanism under the DORA Regulation cannot be changed by the Authority because it is a direct legal requirement emanating from the DORA Regulation itself. Therefore, financial entities will be expected to report incidents pursuant to the DORA Regulation, if they meet the materiality thresholds outlined in the Final Report on the Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554 [note that this Technical Standard has not yet been adopted by the Commission and it is subject to change].

Lastly, and outside of the context of the GDPR, the Authority has taken the necessary steps to ensure that (where possible) no dual incident reporting is required. More specifically in the contexts of Directives (EU) 2015/2366 and (EU) 2022/2555, the Authority takes note that this has been considered as a positive development by respondents to the Public Consultation, as mentioned in the feedback under sub-title '*Centralisation of Incident Reporting*', contained within this Feedback Statement.

Exchange of Information in the Case of Major ICT-related Incidents and Significant Cyber Threats

Feedback Received

Stakeholders asked for clarity in relation to what shall be understood as any other relevant body of authority, in terms of sub-regulation 5 point (3) of the draft *Digital Operational Resilience Act (DORA) Regulations*, reproduced below:

"(3) The Authority shall have the power to disclose any major ICT-related incidents reports and any voluntary notifications of significant cyber threats or any other

*information related thereto to **any other relevant body or authority in accordance with Article 19 of the DORA Regulation** and with article 17 of the Act."*

Authority's Position

Stakeholders are invited to refer to Article 19(6) point (e) of the DORA Regulation, as reproduced below:

*"6. Upon receipt of the initial notification and of each report referred to in paragraph 4, the **competent authority shall**, in a timely manner, provide details of the major ICT-related incident to the following recipients based, as applicable, on **their respective competences**:*

*(e) **other relevant public authorities under national law**."*

Therefore, sub-regulation 5 point (3) directly emanates from Article 19(6) of the DORA Regulation. **Considering the above, the sharing of major ICT-related incident with other relevant public authorities under national law is a requirement being imposed by the DORA Regulation upon the Authority itself.** The circumstances of such sharing are directly related to the competences of the corresponding relevant public authorities under national law.

5. Conclusion

The Authority remains open to requests for clarification and guidance related to the DORA Regulation and the DORA Amending Directive. In this sense, Authorised Persons and interested stakeholders may request further information by sending an email to the Supervisory ICT Risk and Cybersecurity function on sirc@mfsa.mt.