ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

TO : **Regulated Entities:**

i. **Cyprus Investment Firms ('CIFs')**
ii. **Central Securities Depositories**
iii. **Trading Venues**
iv. **Crypto-Asset Providers (CASPs)**
v. **Alternative Investment Fund Managers ('AIFMs')**
vi. **UCITS Management Companies ('UCITS')**

FROM : **Cyprus Securities and Exchange Commission**

DATE : **8 April 2025**

CIRCULAR No : **C700**

SUBJECT : **Digital Operational Resilience Act - Reporting Obligations**
(a) Incident Reporting
(b) Register of Information

The Cyprus Securities and Exchange Commission (the '**CySEC**') issues this circular to inform the Regulated Entities of their reporting obligations under the Digital Operational Resilience Act ('the **DORA**'). The two main reporting requirements are:

A. Incident Reporting – a) Mandatory reporting of major ICT-related incidents and b) Voluntary notification for significant cyber threats.

B. Register of Information - Annual submission of contractual arrangements related to ICT services supporting critical or important functions.

Listed below are the details on how and when these reporting requirements should be submitted to CySEC along with relevant guidance on the framework in place.

A. Incident Reporting

Mandatory reporting of major ICT-related incidents

1. Under Article 19(1) of DORA, Regulated Entities must report major ICT-related incidents to CySEC.

2. When an incident occurs, the Regulated Entity should determine its impact on ICT services and apply the classification criteria laid down in Articles 18(1) of DORA and 1-7 of the Commission Delegated Regulation (EU) 2024/1772 to confirm whether it qualifies as an ICT-related incident.

In particular, according to Article 18(1) of DORA and Articles 1 – 7 of the Commission Delegated Regulation (EU) 2024/1772, Regulated Entities must classify incidents as ICT-related incidents and determine their impact based on the following criteria:

i. the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;
ii. the duration of the ICT-related incident, including the service downtime;
iii. the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;
iv. the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;
v. the criticality of the services affected, including the financial entity's transactions and operations;
vi. the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.

3. If the incident is ICT-related, the Regulated Entity should then evaluate major incident thresholds as specified in Articles 8-9 of the Commission Delegated Regulation (EU) 2024/1772 to determine if it qualifies as a major ICT-related incident.

4. If the event is classified as major, it must be reported to CySEC.

5. Regulated Entities are required to prepare **three sequential reports** - Initial Report, Intermediate Report, and Final Report - for each ICT-related incident using the Major ICT-related incident Form, which includes dedicated sheets for each report.

6. Upon its completion, the Major ICT-related incident Form should be submitted to CySEC within the following deadlines:

i. **Initial report**: Within four hours from the classification of the ICT-related incident as a major ICT-related incident and no later than 24 hours from the moment the Regulated Entity has become aware of the ICT-related incident.

ii. **Intermediate report**: Within 72 hours from the submission of the initial report, even where the status or the handling of the incident have not changed as referred to in Article 19(4), point (b), of DORA. Regulated entities must submit an updated intermediate report without undue delay, and in any case when the regular activities have been recovered.

iii. **Final report**: Within one month after either the submission of the intermediate report, or, where applicable, after the latest updated intermediate report.

7. The Commission Implementing Regulation (EU) 2025/302 provides, among others, standard forms, templates and procedures for financial entities to report a major ICT-related incident.

8. The Commission Delegated Regulation (EU) 2025/301 specifies, among others, the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents.

Voluntary notification for significant cyber threats

9. Under Article 19(2) of DORA, Regulated Entities may, on a voluntary basis, notify significant cyber threats to CySEC when they deem the threat to be of relevance to the financial system, service users or clients.

10. According to Article 18(2) of DORA and Article 10 of the Commission Delegated Regulation (EU) 2024/1772, Regulated Entities must classify cyber threats as significant based on:

i. the criticality of the services at risk,
ii. financial entity's transactions and operations,
iii. number and/or relevance of clients or financial counterparts targeted and
iv. the geographical spread of the areas at risk.

11. Regulated entities should use the Significant Cyberthreats Template (Voluntary) to notify CySEC, on a voluntary basis, regarding significant cyber threats.

12. The Commission Implementing Regulation (EU) 2025/302 provides, among others, standard forms, templates and procedures for financial entities to notify a significant cyber threat.

13. The Commission Delegated Regulation (EU) 2025/301 specifies, among others, the content of the voluntary notification for significant cyber threats.

Submission process of the major ICT-related incident form and the Significant Cyberthreats Template

14. The Major ICT-related incident Form and the Significant Cyberthreats Template (Voluntary) (the 'Incident Reporting Forms') **must be submitted to CySEC through the TRS system ONLY.**

15. The Incident Reporting Forms must **not** be digitally signed.

16. The steps that the Regulated Entities have to follow for the successful submission of the template to the TRS, can be found here. Upon submission, the Regulated Entities are responsible to ensure that they have received a **feedback file**, i.e. an official submission confirmation dispatched by the TRS, in the Outgoing directory.

The feedback file will either contain a NO ERROR indication or, in case that an error(s) has/have occurred during submission, the description of that error(s). In case of any errors detected during submission of the template, Regulated Entities must review the template and ensure that all errors, are addressed and corrected, before they re-submit the template. **The Form is regarded as being successfully submitted to CySEC, only when a NO ERROR indication feedback file is received.**

17. After populating the required Excel fields in the Incident Reporting Forms, Regulated Entities should name the Excel file in accordance with the following naming convention:

For Major ICT-related Incidents:

Username_DATDIR_IIRN-Version_YY.xlsx

For Significant Cyberthreats (Voluntary):

Username_DATCYB_IIRN-Version_YY.xlsx

Where:

i. **Username:** – This Codification is given by CySEC to the Reporting Entities. For Regulated Entities, it is the TRS System username, and it can be found in the TRS/Portal credentials' email which was sent to your Entity. It should be entered in Capital Letters.

ii. **DATDIR** (for Major ICT-related Incidents or **DATCYB** (for Significant Cyberthreats): This is the coding of the Incident Reporting Forms; it should remain unchanged and should be inserted exactly as it appears.

iii. **IIRN**: The Incident Reference Number, a 10-digit code provided by the Reporting Entity; for example, 0123456789. The following should be adhered when completing this field:
   a. this is a unique Sequence Number of 10 digits, and it is incremented each time a Reporting Entity sends a file for a **new** incident.
   b. the sequence should start at 0000000001.
   c. This number identifies uniquely a single incident
   d. The sequence restarts each year.

iv. **Version**: This is the Version field where the following rules apply:
   a. It is used to specify the version of the file for a given sequence number (incident).

b. When the file is been submitted for the first time, then the Version number to be used should be 0, maximum version is 9.
c. Updated files referring to the same incident shall be submitted by the Reporting Entity with an increased version number (previous version number + 1).

v. **YY**: This is a 2-digit code, indicating the current year.

An example of a filename is shown below:

The major ICT related Incident reporting Template: **XX_DATDIR_0000000001-0_25.xlsx**

The Voluntary Significant Template: **XX_DATCYB_0000000001-0_25.xlsx**

18. Due to the entry into force of DORA, CySEC's Circular 512 is repealed.

B. Register of Information

19. Under Article 28(3) of DORA, Regulated Entities must **maintain and update at entity level, and at consolidated level,** a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

Additionally, Regulated Entities **must report** at least yearly to CySEC on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided.

20. According to Article 3, of ESAs' Decision of 8 November 2024 concerning the reporting by competent authorities to the ESAs of information necessary for the designation of critical ICT third-party service providers in accordance with Article 31(1)(a) of Regulation (EU) 2022/2554, the Register of information to be submitted to CySEC should be:

i. at individual entity level, where Regulated Entities are not part of a group of financial entities;
ii. at individual entity level, where Regulated Entities are part of a group of financial entities, and where the parent undertaking is an entity outside of the Union and there is no Union parent undertaking;
iii. at the highest level of consolidation in the Union for groups of Regulated Entities that is available to the competent authorities in accordance with their supervisory responsibilities under the legal acts referred to in Article 46 of Regulation (EU) 2022/2554.

It is noted that the Register of Information will be forwarded to European Supervisory Authorities.

21. Regulated Entities must fill in the Register of Information Form and submit it to CySEC on an annual basis, **by February 28, each year**, with reference date 31 December preceding the reporting date.

For the first submission due the deadline is **Wednesday, April 30, 2025, with a reference date of March 31, 2025.**

22. The Commission Implementing Regulation (EU) 2024/2956 provides standard templates for maintaining and updating the Register of Information

23. In order to provide further guidance for maintaining and updating the Register of Information, the ESAs published guidance and Frequently Asked Questions (FAQ).

Submission process

24. The Register of Information Form should be submitted via CySEC's XBRL Portal ONLY. Once the Template is completed, it should be zipped and submitted, through the Create filing.

25. Regulated Entities may submit an XBRL file.

26. Regulated Entities that have not yet registered in CySEC's XBRL Portal, should do so as soon as possible.

CySEC emphasises that ALL Regulated Entities are required to comply with the abovementioned reporting requirements and ensure timely and accurate submission of the required templates.

For any queries, please contact CySEC in writing via email at prudential@cysec.gov.cy .

Yours sincerely,

Panikkos Vakkou
Vice Chairman
Cyprus Securities and Exchange Commission