L.N. of 2023

MALTA FINANCIAL SERVICES AUTHORITY ACT (CAP. 330)

Malta Financial Services Authority Act (Digital Operational Resilience Act (DORA)) Regulations, 2023

IN EXERCISE of the powers conferred by article 20A of the Malta Financial Services Authority Act, the Minister responsible for the regulation of financial services, acting on the advice of the Malta Financial Services Authority, has made the following regulations:

Citation and scope.

1. (1) The title of these regulations is the Malta Financial Services Authority Act (Digital Operational Resilience Act (DORA)) Regulations, 2023.

(2) The purpose of these regulations is to implement the relevant provisions of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

Interpretation.

2. (1) In these regulations, unless the context otherwise requires:

Cap. 330.

"Act" means the Malta Financial Services Authority Act;

Cap. 330.

"the Authority" means the Malta Financial Services Authority established by the Malta Financial Services Authority Act;

"binding legal instrument" means any directly applicable measures, including, but not limited to, any implementing technical standards, regulatory technical standards or similar measures, issued under European Union legislation;

"CRD" means Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, as amended from time to time, and

includes any binding legal instruments, guidelines and other measures that have been or may be issued thereunder;

"CSIRT" means the Computer Security Incident Response Team designated or established in accordance with Article 10 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) ;

"DORA Regulation" means Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 as may be amended from time to time, and includes any binding legal instruments, guidelines and other measures that have been or may be issued thereunder;

"Minister" means the Minister responsible for the regulation of financial services;

"Threat-Led Penetration Testing" or "TLPT" means a framework that mimics the tactics, techniques and procedures of real- life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems, in terms of Article 3(17) of the DORA Regulation.

(2)(a) Words and expressions used in these regulations which are defined in Article 3 of the DORA Regulation, but which are not defined herein, shall have the same meaning assigned as in the DORA Regulation.

(b) Words and expressions which are also used in the Act which are not defined herein or in Article 3 of the DORA Regulation shall have the same meaning as in the Act.

(c) In the event of any conflict between any of the provisions of these regulations and the provisions of the DORA Regulation, the provisions of the DORA Regulation shall prevail.

Applicability.

Cap. 574.

3. (1) These regulations shall apply to the financial entities referred to in Article 2(1) of the DORA Regulation.

(2) These regulations shall not apply to:

(a) the entities referred to Article 2(3) of the DORA Regulation; and

(b) the Malta Development Bank established in terms of the Malta Development Bank Act.

Competent authority

4. (1) In terms of the relevant provisions of Article 46 of the DORA Regulation, the Authority shall be the designated competent authority in Malta for the purposes of implementing the relevant provisions of the DORA Regulation and for ensuring compliance therewith, and any reference in these regulations to the competent authority shall be read and construed accordingly.

(2) The designation of the Authority as the competent authority under sub regulation (1) shall be without prejudice to:

(a) the European Central Bank (ECB) as the designated competent authority for credit institutions classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, as referred to in Article 46(a) of the DORA Regulation;

(b) the European Securities and Markets Authority (ESMA) as the designated competent authority for credit rating agencies in accordance with Article 21 of Regulation (EU) No 1060/2009, as referred to in Article 46(n) of the DORA Regulation; and

(3) The Authority shall exercise all the functions, obligations and powers, and shall satisfy all the requirements imposed on competent authorities by the DORA Regulation, including the receiving of any reports of any major ICT-related incidents reports and any voluntary notifications of significant cyber threats, in terms of Article 19 of the DORA Regulation.

(4) For the purposes of Article 32(5) of the DORA Regulation, the Authority shall be the relevant competent authority whose staff member shall be the high-level representative for the purposes of Article 32(4)(b) of the DORA Regulation.

(5) Without prejudice to sub-regulation (1) and to any other power conferred on the Authority under any other relevant law, the Authority may, for the better implementation of the DORA Regulation, exercise any of the powers conferred to it under the Act.

(6) In terms of Article 26(10) of the DORA Regulation, without prejudice to the power to identify the financial entities that are required to perform TLPT, the Authority may delegate the exercise of some or all of the tasks referred to in Articles 26 and 27 of the DORA Regulation to another national authority in the financial sector, and any delegation so made shall be published on the Authority's official website without undue delay.

Cooperation and Exchange of Information

5. (1) In the case of receival of any major ICT-related incidents and any voluntary notifications of significant cyber threats made by credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, the Authority shall, in terms of Article 19(1) subparagraph 3 and Article 19(2) subparagraph 2 of the DORA Regulation, immediately transmit the said reports and notifications to the European Central Bank (ECB).

(2) For the purposes of fulfilling its duties and responsibilities as set out in Article 19 of the DORA Regulation, the Authority may transmit to the national CSIRT any major ICT-

related incident reports and any voluntary notifications of significant cyber threats in terms of Article 19 of the DORA Regulation.

(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.

Power of the Authority to issue Rules.

6. The Authority may issue Rules in terms of article 16(2)(a) and article 20A(3) of the Act for the better carrying out of the provisions of these regulations and the DORA Regulation.

Supervisory powers of the Authority.

7. Without prejudice to any other power assigned to the Authority under the Act, these regulations, the DORA Regulation and any other law, the Authority shall also have the power to:

(a) access to any document or data held in any form that the Authority considers relevant for the performance of its duties and receive or take a copy of it;

(b) carry out on-site inspections or investigations, which shall include:

i) summoning representatives of the financial entities for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers; and

ii) interviewing any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;

(c) require corrective and remedial measures for breaches of the requirements of the DORA Regulation, the Act, these regulations or any other regulations or rules issued thereunder which implement the DORA Regulation:

Provided that any decision so taken under this paragraph shall be properly reasoned:

Provided further that where such corrective and remedial measures are taken with respect to a legal person, the Authority shall have the power to apply the said corrective and remedial measures, subject to any conditions that may be provided for in any other law, to members of the management body, and to other individuals who under national law are responsible for the breach.

The Authority's powers to impose administrative penalties and other administrative measures.

8. (1) Without prejudice to any other power of the Authority conferred to it under the DORA Regulation, the Act or any regulations issued thereunder, including these regulations, where the Authority is satisfied that a person's conduct amounts to a breach of any of the provisions of the DORA Regulation, the Act, these regulations, or of any regulations or Rules made thereunder and implementing the provisions of the DORA Regulation, or otherwise that a person has contravened or failed to comply with any condition, obligation, requirement, order or directives made or given by the Authority under any of the provisions thereof, including failure to cooperate in an investigation or an on-site inspection, the Authority may, by notice in writing and without recourse to a court hearing, impose on any such person administrative measures and, or administrative penalties which may not exceed one hundred and fifty thousand Euro (€150,000) for each infringement or failure to comply, as the case may be. The provisions of article 16(4) of the Act shall apply *mutatis mutandis*.

(2) Without prejudice to the generality of sub-regulation (1), the Authority shall also have the power to impose the following administrative penalties and administrative measures for any breach of any of the provisions of the DORA Regulation, the Act, these regulations and any regulations or rules issued thereunder implementing the DORA Regulation:

(a) issue an order requiring the natural or legal person to cease the conduct in breach of the DORA Regulation, the Act, any regulations or rules issued thereunder implementing the DORA Regulation, and to desist from a repetition of that conduct;

(b) require the temporary or permanent cessation of any practice or conduct that the Authority considers to be contrary to the provisions of the DORA Regulation, the Act, any regulations or Rules issued thereunder implementing the DORA Regulation, and prevent repetition of that practice or conduct;

(c) adopt any type of measure, including of a pecuniary nature, permitted in terms of the DORA Regulation, the Act or these Regulations, to ensure that financial entities in terms of the DORA Regulation continue to comply with their legal requirements;

(d) require existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of the DORA Regulation, the Act, these regulations and any regulations or rules issued thereunder implementing the DORA Regulation, and where such records may be relevant to an investigation into such breaches; and

(e) issue public notices, including public statements, which indicate the identity of the natural or legal person and the nature of the breach:

Provided that where administrative penalties and administrative measures are taken in terms of this sub-regulation with respect to a legal person, the Authority shall have the power to apply such penalties and measures, subject to any conditions that may be provided for in any other law, to members of the management body, and to other individuals who under national law are responsible for the breach.

(3) Administrative penalties and other administrative measures imposed by the Authority shall be effective, proportionate and dissuasive.

(4) When determining the type and level of an administrative penalty or other administrative measures to be imposed under these regulations , the Authority shall take into account the extent to which the breach is intentional or results from negligence, and all the relevant circumstances, including, where appropriate:

(a) the materiality, gravity and the duration of the breach;

(b) the degree of responsibility of the natural or legal person responsible for the breach;

(c) the financial strength of the natural or legal person responsible for the breach;

(d) the importance of profits gained or losses avoided by the natural or legal person responsible for the breach, insofar as they can be determined;

(e) the losses for third parties caused by the breach, insofar as they can be determined;

(f) the level of cooperation with the competent authority of the natural or legal person responsible for the breach, without prejudice to the need to ensure disgorgement of profits gained or losses avoided by such person; and

(g) previous breaches by the natural or legal person responsible for the breach.

(5) The imposition by the Authority of an administrative penalty or administrative measure in terms of these regulations shall be without prejudice to any other consequence of the act or omission of the offender under civil or criminal law:

Provided that in all cases where the Authority imposes an administrative penalty or administrative measure in respect of anything done or omitted to be done by any person and such act or omission also constitutes a criminal offence, no proceedings may be taken or continued against the said person in respect of such criminal offence.

Publication of administrative penalties and other administrative measures.

9. (1) The Authority shall publish any decision imposing an administrative penalty or other administrative measures which it shall take under these regulations, on its official website, without undue delay, after the person on whom the penalty was imposed has been notified of that decision. The publication shall include information on the type and nature of the breach the identity of the persons responsible and the administrative penalty or other administrative measures imposed:

Provided that where the Authority publishes a decision imposing an administrative penalty or other administrative measures against which there is an appeal before the Financial Services Tribunal or the relevant judicial authorities, the Authority shall immediately add on its official website that information and, at later stages, any subsequent related information on the outcome of such appeal:

Provided further that any decision of the Financial Services Tribunal or other judicial decision annulling a decision of the Authority imposing an administrative penalty or other administrative measures shall also be published.

(2) Where the Authority, following a case-by-case assessment, considers that the publication of the identity of legal persons or of the identity and personal data of natural persons, as the case may be, would:

(a) be disproportionate, including risks in relation to the protection of personal data;

(b) jeopardise the stability of financial markets;

(c) jeopardise the pursuit of an ongoing criminal investigation; or

(d) cause, insofar as these can be determined, disproportionate damages to the person involved;

the Authority shall adopt one of the following solutions in respect of the decision imposing an administrative penalty or other administrative measures:

(aa) defer the publication of the decision until all the reasons for non-publication cease to exist;

(bb) publish the decision on an anonymous basis; or

(cc) refrain from publishing the decision, where the options referred to in paragraphs (aa) and (bb):

(i) are considered to be insufficient to guarantee a lack of any danger for the stability of financial markets; or

(ii) where such publication would be disproportionate to the leniency of the imposed administrative penalty or other administrative measures.

(3) In the case of a decision to publish an administrative penalty or other administrative measures on an anonymous basis in terms of paragraph (bb) of sub-regulation (2), the publication of the relevant data may be postponed.

(4) The Authority shall ensure that any publication in accordance with this regulation shall remain on its official website only for the period which is necessary to bring forth this regulation:

Provided that this period shall not exceed five (5) years after its publication.

Right of appeal.

10. Subject to the provisions of the Act, any person in respect of whom a decision is taken by the Authority under the Act, these regulations or the DORA Regulation, may appeal to the Financial Services Tribunal in terms of article 21 of the Act and the provisions of the said article 21 shall *mutatis mutandis* apply.

Offences.

11. (1) Any person who –

(a) fails to comply with any order or directive issued by the Authority under the DORA Regulation, the Act, these regulations or any regulations issued thereunder which implement the DORA Regulation; or

(b) without reasonable excuse alters, suppresses, conceals, destroys or refuses to produce any document which he is lawfully required to produce under the DORA Regulation, the Act, these regulations or any regulations made or rules issued thereunder which implement the DORA Regulation; or

(c) for the purposes of, or pursuant to, any of the provisions of the DORA Regulation, the Act, these regulations or of any regulations or Rules issued thereunder, or any condition, obligation, requirement, directive or order made or given as aforesaid, furnishes information or makes a statement which he knows to be inaccurate, false or misleading in any material respect, or recklessly furnishes information or makes a statement which is inaccurate, false or misleading in any material respect; or

(d) intentionally obstructs a person from exercising rights or powers conferred by the DORA Regulation, the Act, these regulations or any regulations issued under the Act; or

(e) contravenes or fails to comply with any of the provisions of the DORA Regulation, the Act, these regulations or any regulations made or rules issued thereunder which implement the DORA Regulation;

shall, on conviction, be liable to the punishment of imprisonment for a term not exceeding one year or to a fine (*multa*) not exceeding one hundred and fifty thousand Euro (€150,000) or to both such fine and imprisonment.

(2) The provisions of the Act or these regulations shall not affect any criminal proceedings that may be competent under any other law.

(3) The Authority shall have the power to:

(a) liaise with the Commissioner of Police to receive specific information related to criminal investigations or proceedings commenced for breaches of the DORA Regulation. The Commissioner of Police shall cooperate with the Authority, thereby providing such specific information related to any criminal investigations or proceedings commenced in relation to such breaches; and

(b) provide the same information received in terms of paragraph (a), and transmit copies of acts and documents of the courts of criminal justice in terms of the second proviso to article 518 of the Criminal Code, to other authorities which are deemed competent authorities for the purposes of Article 46 of the DORA Regulation, as well as to the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) or the European Insurance and Occupational Pensions Authority (EIOPA), for the purpose of fulfilling its obligations to cooperate for the purposes of the DORA Regulation and these regulations.