L.N. 216 of 2018

EUROPEAN UNION ACT
(CAP. 460)

Measures For High Common Level of Security of Network and Information Systems Order, 2018

IN EXERCISE of the powers conferred by article 4(2) of the European Union Act, the Prime Minister has made the following order:-.

PART I - PRELIMINARY

Citation and scope.

1. (1) The title of this order is Measures for High Common Level of Security of Network and Information Systems Order, 2018.

(2) This order transposes Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Interpretation.

2. In this order unless the context otherwise requires:

"autonomous CSIRT" means a self-organised CSIRT which provides a monitoring function of CSIRT services and alerts to its own business or other agencies, operators of essential services or digital service providers;

S.L. 460. 24

"CIP Unit" means the Malta Critical Infrastructure Protection (CIP) Unit established under article 3 of the Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order;

"CIIP Unit" means the Critical Information Infrastructure Protection Unit as established under article 5(1);

"cloud computing service" means a digital service that enables access to a scalable and elastic pool of shareable computing resources;

"consumer" means any natural person who is acting for purposes which are outside his trade, business, craft or profession;

"critical information infrastructure" or "CII" means an information and communication technology asset, system, network or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of

people, and the disruption or destruction of which would have a significant impact in Malta as a result of the failure to maintain those functions;

"critical infrastructure" or "CI" has the same meaning assigned to it by article 2 of the Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order; S.L. 460. 24.

"CSIRT" means computer security incident response team;

"Data Protection Commissioner" means the Information and Data Protection Commissioner as appointed under article 11 of the Data Protection Act. Cap. 586.

"digital service" means a service within the meaning of regulation 2 of the Notification Procedure Regulations which is of a type listed in the Third Schedule; S.L. 419.06.

"DNS service provider" means an entity which provides DNS services on the internet;

"digital service provider" means any legal person that provides a digital service;

"domain name system" or "DNS" means a hierarchical distributed naming system in a network which refers queries for domain names;

"incident" means any event having an effect on the security of network and information systems;

"incident handling" means all procedures supporting the detection, analysis and containment of an incident and the response thereto;

"internet exchange point" or "IXP" means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

"Malta Communications Authority" means the authority established under article 3 of the Malta Communications Authority Act; Cap. 418.

"Member States" means the Member States of the European

Union;

"Minister" means the Minister responsible for the protection of critical infrastructure and critical information infrastructure protection;

"national strategy on the security of network and information systems" means a framework providing strategic objectives and priorities on the security of network and information systems at national level;

"network and information system" means:

Cap. 399.

(a) an electronic communications network within the meaning of article 2 of the Electronic Communications (Regulation) Act;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under paragraphs (a) and (b) for the purposes of their operation, use, protection and maintenance.

"online marketplace" means a digital service that allows consumers, traders or both as respectively defined in paragraph (a) and in paragraph (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council to conclude online sales or services contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace*;*

"online search engine" means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

"operator of essential services" means a public or private entity of a type referred to in the Second Schedule, which meets the criteria laid down in article 9(2);

"operator security plan" or "business continuity management" is the overall procedure identifying the assets, systems, networks or part thereof within critical information infrastructures, operator of essential services and, or digital service providers, identifying the security solutions and technical measures that exist or are being implemented for their protection and the identification, selection and prioritization

of counter measures and procedures;

"representative" means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this order;

"risk" means any reasonably identifiable circumstance or event having a potential effect on the security of network and information systems and leading to uncertainty on the objectives of an asset, system, network or part thereof. An effect is a deviation from the expected objectives, objectives may have different aspects and may apply at different levels, positive or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk is often characterized by reference to potential events and consequences, or a combination of these. Risk is often expressed in terms of a combination of the consequences of an event, including changes in circumstances, and the associated likelihood of occurrence;

"risk assessment" is the overall process of risk identification, risk analysis and risk evaluation, incorporating the identification of risk sources, events, their causes and their potential consequences, comprehending the nature of risk and determining the level of risk, with the ultimate objective of comparing the results of the risk analysis with the risk criteria in order to determine whether the risk and, or its magnitude is acceptable or tolerable;

"security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via those network and information systems;

"standard" means a standard within the meaning of paragraph (1) of Article 2 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council;

"specification" means a technical specification within the meaning of paragraph (4) of Article 2 of Regulation (EU) No 1025/ 2012 of the European Parliament and of the Council;

"top-level domain name registry" means an entity which

administers and operates the registration of internet domain names under a specific top-level domain;

"trader" means any natural persons, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession;

Cap. 460.

"Treaty" shall have the same meaning as in article 2 of the European Union Act.

Applicability.

3. (1) The security and notification requirements of this order shall not apply to undertakings which are subject to the requirements of Article 13a and 13b of Directive 2002/21/EC of the European Parliament and of the Council, or to trust service providers which are subject to requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council.

S.L. 460.24.

(2) This order applies without prejudice to the Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order and Directives 2011/93/EU and 2013/40/EU of the Europe Parliament and of the Council.

(3) Without prejudice to Article 346 TFEU, information that is confidential pursuant to law, such as rules on business confidentiality, shall be exchanged with the European Commission and relevant authorities only where such exchange is necessary for the application of this order. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of operators of essential services and digital service providers.

(4) This order is without prejudice to the actions taken to safeguard essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which is contrary to the essential interests of the security of Malta, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

(5) Where a sector-specific law requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this order, those provisions of that sector-specific law shall apply.

4. Processing of personal data pursuant to this order shall be carried out in accordance with the Data Protection Act and Regulation 2016/679/EU of the European Parliament and of the Council. Processing of personal data. Cap. 586.

PART II – CRITICAL INFORMATION INFRASTRUCTURE PROTECTION UNIT, CSIRTMalta and CSIRTs

5. (1) There shall be a Critical Information Infrastructure Protection Unit within the Critical Infrastructure Protection Directorate, herein referred to as the 'CIIP Unit'. The CIIP Unit.

(2) The CIIP Unit shall be responsible for monitoring the application of this order and shall be the national competent authority covering the sectors referred to in the Second Schedule and the services referred to in the Third Schedule.

(3) The CIIP Unit shall be responsible for:

(a) establishing the criteria for the identification and designation of operators of essential services and digital service providers;

(b) identifying and designating operators of essential services within Malta pursuant to article 9;

(c) identifying the services provided by operators of essential services and digital service providers;

(d) ensuring that a risk assessment is carried out by operators of essential services and digital service providers;

(e) ensuring that operators of essential services and digital service providers draw up and maintain an operator security plan;

(f) instigating simulated runs of operator security plans by operators of essential services and digital service providers.

(g) without prejudice to article 3(3), building partnerships with operators of Critical Information Infrastructures (CIIs) for information sharing;

(h) maintaining a register of CSIRTs, operators of essential services and digital service providers providing services in Malta;

(i) exercising a liaison function to ensure cross-border cooperation with the relevant authorities in other Member States

and with the Cooperation Group and the CSIRTs network;

(j) adopting a national strategy on the security of network and information systems pursuant to article 8;

(k) monitoring security measures taken by operators of essential services pursuant to article 11.

(4) The CIIP Unit shall also perform such related and consequential duties as the Minister may delegate from time to time.

(5) The CIIP Unit shall, whenever appropriate and in accordance with law, consult and cooperate with the relevant national law enforcement authorities and the Data Protection Commissioner.

CSIRTs.

6. (1) There shall be a National CSIRT within the CIIP Unit, to be known as CSIRTMalta which shall comply with the requirements and tasks set out in paragraphs 1 and 2 of the First Schedule respectively, covering at least the sectors referred to in the Second Schedule and the services referred to in the Third Schedule. CSIRTMalta shall be responsible for risk and incident handling in accordance with a well-defined process.

(2) CSIRT Malta shall inform the CIIP Unit about incident notifications submitted pursuant to this order.

(3) Operators of an essential service shall receive CSIRT monitoring services from any of the following CSIRTs which shall comply with the requirements and tasks set out in paragraphs 1 and 3 respectively of the First Schedule:

(a) an internal CSIRT providing CSIRT monitoring services and alerts within operators of essential services;

(b) an autonomous CSIRT may be contracted to perform CSIRT monitoring services.

(4) Any operator of essential services which fails to establish a CSIRT as provided for in sub-article (3) shall be liable to an administrative fine in accordance with the procedure under article 19.

(5) The CIP Unit and CIIP Unit shall cooperate for the better fulfilment of the obligations laid down in this order.

Resources.

7. The Minister shall ensure that:

(a) the CIIP Unit and CSIRTMalta have adequate resources to carry out in an effective and efficient manner, the

tasks assigned to them and thereby to fulfil the objectives of this order;

(b) CSIRTMalta shall have access to an appropriate, secure and resilient communication and information infrastructure at national level.

PART III– NATIONAL FRAMEWORK ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

National Strategy on the security of network and information systems.

8. The CIIP Unit in collaboration with other entities and stakeholders, shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in the Second Schedule and the services referred to in the Third Schedule. The national strategy on the security of network and information systems shall address, in particular, the following issues:

(a) the objectives and priorities of the national strategy on the security of network and information systems;

(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;

(c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;

(d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;

(e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;

(f) a risk assessment plan to identify risks;

(g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

PART IV – SECURITY OF NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICE

Identification of operators of essential services.

9. (1) The CIIP Unit shall for each sector and subsector referred to in the Second Schedule identify operators of essential services within Malta.

(2) In identifying operators of essential services pursuant to sub-article (1) the CIIP unit shall take into account that:

(a) the entity provides a service which is essential for the maintenance of critical societal, economic activities or both;

(b) the provision of that service depends on network and information systems; and

(c) an incident would have significant disruptive effects on the provision of that service.

(3) For the purposes of sub-article (1), the CIIP Unit shall establish a list of the services referred to in paragraph (a) of sub-article (2).

(4) Upon a request in writing by the CIIP Unit, a potential operator of essential services in Malta shall within twenty (20) days provide a list of essential services it provides.

(5) The CIIP Unit shall review the list provided pursuant to sub-article (4), and inform the potential operator of essential services whether it has been designated as an operator of essential services pursuant to this article within reasonable time.

(6) A designated operator of essential services shall comply with the designation notification referred to in sub-article (5) within a stipulated time as may be directed by the CIIP Unit.

(7) Any undertaking which fails to comply with the CIIP Unit's request pursuant to sub-article (4) shall be liable to an administrative fine in accordance with the procedure under article 19.

(8) The CIIP Unit shall on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.

Significant disruptive effect.

10. (1) When determining the significance of a disruptive effect as referred to in article 9(2)(c), the CIIP Unit shall take into account at least the following cross-sectoral factors:

(a) the number of users relying on the service provided by the entity concerned;

(b) the dependency of other sectors referred to in the Second Schedule on the service provided by that entity;

(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;

(d) the market share of that entity;

(e) the geographic spread with regard to the area that could be affected by an incident;

(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service;

(g) the dependency of a critical infrastructure, critical information infrastructure, or both, on the service provided by that entity.

(2) In order to determine whether an incident would have a significant disruptive effect, the CIIP Unit shall also, where appropriate, take into account sector-specific factors.

Security requirements and incident notification.

11. (1) The CIIP *Unit* shall ensure that operators of essential services:

(a) take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed;

(b) take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services; and

(c) appoint a security liaison officer who shall have the necessary expertise and who shall:

(i) facilitate the development, implementation, maintenance and review of an operator of essential services

preparedness, processes and solutions;

(ii) ensure that an operator of essentials services conducts and maintains appropriate risk assessments;

(iii) ensure that the operator of essential services maintains and exercises an operator security plan; and

(iv) act as the point of contact for security related issues for ensuring the fulfilment of the obligations laid down in this order between the operator of essential services and the Critical Information Infrastructure Protection (CIIP) Unit.

(2) Operators of essential services shall notify the CIIP Unit, without undue delay, of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the CIIP Unit to determine, any local or cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

(3) In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

(a) the number of users affected by the disruption of essential service;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the sectors affected by the disruption of essential service;

(e) the dependency of a critical infrastructure, critical information infrastructure, or both, on the disruption of essential services.

(4) On the basis of the information provided in the notification by the operator of essential services, the CIIP Unit shall, inform the other affected Member States if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the CIIP Unit, in accordance with law, shall preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

Where the circumstances allow, the CIIP Unit shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.

The CIIP Unit shall forward notifications as referred to in the first paragraph to single points of contact of other affected Member States.

(5) Where a designated operator of essential services provides a service to an undertaking providing electronic communications networks and, or services in terms of the Electronic Communications (Regulation) Act, any security breach affecting such operator of essential services shall also be notified by the relevant CSIRT to the Malta Communications Authority: Cap. 399.

Provided that in this context, in exercising their regulatory oversight, the CIIP Unit and the Malta Communications Authority shall consult each other and each shall give due consideration to any advice that the other may give.

(6) After consulting the notifying operator of essential services, the CIIP Unit may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

(7) Any operator of essential services which fails to comply with the obligations of this article shall be liable to an administrative fine in accordance with the procedure under article 19.

12. (1) The Minister shall ensure that the CIIP Unit has the necessary powers and means to assess the compliance of operators of essential services with their obligations under article 11 and the effects thereof on the security of network and information systems. Implementation and enforcement.

(2) Upon the request of the CIIP Unit, operators of essential services shall without undue delay provide:

(a) the information necessary to assess the security of their network and information systems, including documented security policies;

(b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the CIIP Unit or a qualified auditor and, in the latter case to make the results thereof, including the underlying evidence, available to the CIIP Unit.

When requesting such information, the CIIP Unit shall state the purpose of the request and specify what information is needed.

(3) Following the assessment of information, evidence or results of security audits referred to in sub-article (2), the CIIP Unit may issue binding instructions to the operators of essential service to remedy the deficiencies identified.

(4) The CIIP Unit shall work in close cooperation with the Data Protection Commissioner when addressing incidents resulting in personal data breaches.

PART V – SECURITY OF NETWORK AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS

Security requirements and incident notification.

13. (1) Digital service providers shall identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services within Malta referred to in the Third Schedule. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) monitoring, auditing and testing;

(e) compliance with international standards.

(2) Digital service providers shall take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in the Third Schedule that are offered within Malta, with a view to ensuring the continuity of those services.

(3) Digital service providers shall without undue delay, notify the CIIP Unit of any incident having a substantial impact on the provision of a service as referenced in the Third Schedule that they offer within Malta. Notifications shall include information to enable the CIIP Unit to determine the significance of any local and cross-border impact. Notification shall not make the notifying party subject to increased liability.

(4) In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

(e) the extent of the impact on economic and societal activities;

(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service;

(g) the dependency of a critical infrastructure, critical information infrastructure, or both, on the service provided by that entity.

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first paragraph.

(5) Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified in writing and without undue delay by that operator.

(6) Where appropriate, and in particular if the incident referred to in sub-article (3) concerns two or more Member States, the CIIP Unit shall inform the competent authority or CSIRT of the other affected Member States. In so doing, the CIIP Unit shall, in accordance with the law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

(7) After consulting the digital service provider concerned, the

CIIP Unit, where appropriate, may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

(8) Without prejudice to article 3(4), the CIIP Unit shall not impose any further security or notification requirements on digital service providers.

(9) Part V shall not apply to micro and small enterprises as defined in Commission Recommendation 2003/361/EC.

(10) Any digital service provider which fails to comply with the obligations set out in this article shall be liable to the imposition of an administrative fine in accordance with the procedure under article 19.

Implementation and enforcement.

14. (1) The CIIP Unit shall take action, if necessary, through *ex post* supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in article 13. Such evidence may be submitted by a competent authority of another Member State where the service is provided by the digital service provider itself.

(2) For the purposes of sub-article (1), the CIIP Unit shall have the necessary powers and means to require digital service providers to:

(a) provide the information necessary to assess the security of their network and information systems, including documented security policies;

(b) remedy any failure to meet the requirements laid down in article 13.

(3) Where:

(a) a digital service provider has its main establishment or a representative in Malta, but its network and information systems is located in one or more Member States; or

(b) a digital service provider has its main establishment or a representative in a Member State, but its network and information systems is located in Malta,

the CIIP Unit shall cooperate and assist competent authorities of other Member States as necessary. Such assistance and cooperation may cover information exchanges between the CIIP Unit and other Member State competent authorities concerned and requests to take supervisory

measures referred to in sub-article (2).

Malta Communications Authority. Cap. 399.

15. Where a designated digital service provider provides a service to an undertaking providing electronic communications networks and services in terms of the Electronic Communications (Regulation) Act, any security breach affecting such digital service provider shall also be notified by the relevant CSIRT to the Malta Communications Authority:

Provided that in this context, in exercising their regulatory oversight, the CIIP Unit and the Malta Communications Authority shall consult each other and each shall give due consideration to any advice that the other may give.

Jurisdiction and territoriality.

16. (1) For the purposes of this order, a digital service provider shall be deemed to be under the jurisdiction of Malta if it has its main establishment in Malta. A digital service provider shall be deemed to have its main establishment in Malta when it has its head office in Malta.

(2) A digital service provider that is not established in the Union, but offers services referred to in the Third Schedule within the Union, shall be deemed to be under the jurisdiction of Malta where its representative is established in Malta.

(3) The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.

PART VI - STANDARDISATION AND VOLUNTARY NOTIFICATION

Standardisation.

17. In the implementation of article 11(1) and article 13 (1) and (2), the CIIP Unit shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

Voluntary notification.

18. (1) Entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

(2) When processing notifications, the CIIP Unit shall act in accordance with the procedure set out in article 11 and may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on the CIIP

Unit.

Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.

PART VII – ENFORCEMENT AND SANCTIONS

Enforcement.

19. (1) The CIIP Unit may take the following measures in respect of any undertaking which infringes any provision of this order or of any other law which the CIIP Unit is entitled to enforce, or who fails to comply with any decision given by the CIIP Unit:

(a) the imposition of an administrative fine in accordance with the provisions of this article; and

(b) order the cessation of any act or omission which is in breach of this order.

(2) The CIIP Unit shall, before proceeding to take any of the measures under sub-article (1), write to the undertaking concerned, warning it of the measure that may be taken and the specific reason why it may be taken, requiring it to cease or rectify its acts or omissions and, or to make its submissions thereto within such period not being less than fifteen (15) days which period, without prejudice to the provisions of sub-article (4), may be abridged if the CIIP Unit considers that the continuance of the infringement impacts negatively the effective exercise by the CIIP Unit of its regulatory functions and, or warrants the immediate intervention of the CIIP Unit:

Provided that where the measure is an administrative fine the undertaking concerned shall also be informed of the amount of the fine:

Provided further that when issuing a warning under this sub-article, the CIIP Unit may impose such conditions as it may consider reasonable in the circumstances.

(3) If the undertaking concerned remedies the infringement within the period established by the CIIP Unit in accordance with sub-article (2), and agrees in writing to abide with any condition that the CIIP Unit may impose, the CIIP Unit may at its discretion desist from proceeding any further, this without prejudice to any regulatory measures that may have already been imposed.

(4) If after the lapse of the period mentioned in sub-article (3), the CIIP Unit considers that the undertaking concerned has not given any valid reasons to demonstrate why no measure should be taken

against it, the CIIP Unit shall notify the undertaking concerned in writing, specifying the nature of the infringement, stating the measure being taken, and if the measure is an administrative fine, stating the amount of the fine being imposed.

(5) Notwithstanding the provisions of sub-article (2), where the CIIP Unit has *prima facie* evidence that the infringement represents an immediate and significant disruptive effect in Malta, the CIIP Unit may take urgent interim measures to remedy the situation in advance of reaching a final decision, including ordering the immediate cessation of the act or omission giving cause to the infringement:

Provided that the undertaking which is subject to such contemplated measures, shall, thereafter, be given a reasonable opportunity to state its view and propose any remedies:

Provided further that the interim measures shall be valid for a maximum of three months, subject to extension for a further period of three months, in circumstances where enforcement procedures have not been completed.

(6) The notification as referred to in sub-article (4) shall, upon the expiry of the time limit for appeal therefrom, upon the service of a copy thereof by means of a judicial act on the undertaking indicated in the notice, constitute an executive title for all effects and purposes of Title VII of Part I of Book Second of the Code of Organization and Civil Procedure: Cap. 12.

Provided that if the undertaking against which the notice has been issued, files an appeal before the Tribunal within the twenty (20) day period referred to under article 22, and concurrently with or before the filing of its appeal requests the Tribunal to suspend the effects of the notice, then the CIIP Unit shall desist from issuing a judicial act as referred to in this sub-article until such time as the request for suspension has been determined, withdrawn or otherwise dealt with:

Provided further that the Tribunal shall determine any requests for suspension referred to in this sub-article expeditiously. Before determining any such request the Tribunal shall give the CIIP Unit a reasonable opportunity to reply and make its submissions.

(7) The effect of a decision of the CIIP Unit to which an appeal relates shall not, except where the Tribunal so orders, be suspended in consequence of the bringing of the appeal.

Quantum of an administrative fine.

20. (1) An undertaking which, fails to:

(a) implement appropriate and proportionate security measures pursuant to article 11 and 13; or

(b) fails to cooperate with the CIIP Unit when exercising its monitoring obligations under this order,

shall be liable to an administrative fine of not less than one thousand euro (€1000) and not more than one hundred thousand euro (€100,000) for each violation and one hundred euro (€100) for each day during which such violation persists, which fine shall be determined and imposed by the CIIP Unit, in accordance with the procedure under article 19:

Provided that any daily fine imposed may be backdated to the date of the commission or commencement of the infringement.

(2) An undertaking which:

(a) fails to notify where it ought to have notified an incident;

(b) fails to comply with a lawful instruction from the CIIP Unit; or

(c) fails to comply with the provisions of this order other than those listed under sub-article (1);

shall be liable to an administrative fine of not less than five hundred euro (€500) and not more than fifty thousand euro ((€50,000) for each violation and fifty euro (€50) for each day during which such violation persists, which fine shall be determined and imposed by the CIIP Unit, in accordance with the procedure under article 19:

Provided that any daily fine imposed may be backdated to the date of the commission or commencement of the infringement.

(3) In determining the amount of an administrative fine, regard shall be had in particular to the nature and extent of the infringement, its duration and the impact on critical societal and economic activities.

PART VIII ADMINISTRATIVE REVIEW TRIBUNAL

Administrative Review Tribunal.

21. (1) The Administrative Review Tribunal shall be competent to hear and determine appeals from decisions of the CIIP Unit as provided in this order or in any law.

(2) The provisions of the Administrative Justice Act, in so far as they apply to the Administrative Review Tribunal, shall apply to any proceedings before the said Tribunal and the words 'public administration' in the said enactment shall be construed as a reference to the CIIP Unit. Cap. 490.

22. (1) The right to appeal to the Tribunal shall be competent to any undertaking to which the decision is addressed. Appeals from decisions.

(2) An appeal from a decision of the CIIP Unit shall be made by application and shall be filed with the Secretary of the Tribunal within twenty (20) days from the date on which the said decision has been notified.

23. In determining an appeal the Tribunal shall take into account the merits of the appeal, and may in whole or in part, confirm or annul the decision appealed from, giving in writing the reasons for its decision and shall cause such decision to be made public and communicated to the parties to the appeal. Decisions of the Tribunal.

FIRST SCHEDULE

REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and, or regulation. Such requirements and tasks shall include the following:

(1) Requirements for all CSIRTs:

(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

(b) CSIRTs' premises and the supporting information systems shall be located in secure sites.

(c) Operator Security and Business continuity:

(i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.

(ii) CSIRTs shall be adequately staffed with computer security incident response officers (CSIROs) to ensure availability at all times.

(iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.

(d) CSIRTs shall have the possibility to participate, where they wish to do so, in local, international cooperation networks or both.

(2) CSIRTMalta’s tasks:

(a) CSIRTMalta tasks shall include at least the following:

(i) monitoring incidents at a national level;

(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(iii) Coordinating and responding to incidents providing the necessary support and advice to constituents;

(iv) providing dynamic risk and incident analysis and situational awareness;

(v) participating in the CSIRTs network and in the European Cooperation Group to ensure the effective, efficient and secure cooperation at the European level;

(b) CSIRTMalta shall establish cooperation relationships with the public and private sector.

(c) To facilitate cooperation, CSIRTMalta shall promote the adoption and use of common or standardised practices for:

(i) incident and risk-handling procedures;

(ii) incident, risk and information classification schemes;

(3) CSIRTs' tasks:

(a) CSIRTs' tasks shall include at least the following:

(i) monitoring incidents of assets, systems, or networks;

(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(iii) responding to incidents;

(iv) providing dynamic risk and incident analysis and situational awareness.

SECOND SCHEDULE

TYPES OF ENTITIES FOR THE PURPOSES OF THE INTERPRETATION OF "OPERATOR OF ESSENTIAL SERVICES" UNDER ARTICLE 2

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive
		Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC
		Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC
	(b) Oil	Operators of oil transmission pipelines
		Operators of oil production, refining and treatment facilities, storage and transmission
	(c) Gas	Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council ([2])
		Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC
		Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC
		Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC
		LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC
		Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		Operators of natural gas refining and treatment facilities

2. Transport	(a) Air transport	Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council ([3])
		Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council ([4]), airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in point 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council ([5]), and entities operating ancillary installations contained within airports
		Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council ([6])
	(b) Rail Transport	Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council ([7])
		Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water transport	Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council ([8]), not including the individual vessels operated by those companies
		Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council ([9]), including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council ([10])

	(d) Road transport	Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ([11]) responsible for traffic management control
		Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council ([12])
3. Banking		Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council ([13])
4. Financial market infrastructures		Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council ([14])
		Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council ([15])
5. Health sector	Health care settings (including hospitals and private clinics)	Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council ([16])
6. Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC ([17]) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services
7.Digital Infrastructure		IXPs
		DNS service providers
		TLD name registries
8. Public Administration		Government Departments, entities, assets, systems and networks within the public service and public sector.

([1]) Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (OJ L 211, 14.8.2009, p. 55).

([2]) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

([3]) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

([4]) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

([5]) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans–European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

(6) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).

([7]) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).

([8]) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

([9]) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

([10]) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

([11]) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21).

([12]) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

([13]) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

([14]) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

([15]) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

([16]) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45).

([17]) Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

THIRD SCHEDULE

TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF THE INTERPRETATION OF "DIGITAL SERVICE" UNDER ARTICLE 2

1. Online marketplace.

2. Online search engine.

3. Cloud computing service.

Ippubblikat mid-Dipartiment tal-Informazzjoni (doi.gov.mt) — Valletta — ***Published by the Department of Information (doi.gov.mt) — Valletta***
Mitbugħ fl-Istamperija tal-Gvern fuq karta FSC — ***Printed at the Government Printing Press on FSC certified paper***

Prezz/*Price*
€2.43