SECOND SUPPLEMENT TO THE GIBRALTAR GAZETTE

No. 4460 of 08 May, 2018

LEGAL NOTICE NO. 102 OF 2018.

CIVIL CONTINGENCIES ACT 2007

INTERPRETATION AND GENERAL CLAUSES ACT

CIVIL CONTINGENCIES ACT 2007 (AMENDMENT) REGULATIONS 2018

ARRANGEMENT OF REGULATIONS

Regulation

LEGAL NOTICE NO. 102 OF 2018.

CIVIL CONTINGENCIES ACT 2007

INTERPRETATION AND GENERAL CLAUSES ACT

CIVIL CONTINGENCIES ACT 2007 (AMENDMENT) REGULATIONS 2018

In exercise of the powers conferred on it by section 31 of the Civil Contingencies Act 2007, as read with section 23(g) (i) of the Interpretation and General Clauses Act, and in order to transpose 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 European Union, the Government has made the following Regulations -

Title and commencement.

1.(1) These Regulations may be cited as the Civil Contingencies Act 2007 (Amendment) Regulations 2018.

(2) These Regulations come into force on 10th May 2018.

Amendment of the Civil Contingencies Act 2007.

2.(1) The Civil Contingencies Act 2007 (in these Regulations referred to as the "**Act**") is amended in accordance with regulations 3 to 6.

Insertion of Part 7.

3. The Act is amended by inserting the following Part after Part 6 -

"PART 7

SECURITY OF NETWORK AND INFORMATION SYSTEMS

Overview.

32.(1) This Part makes provision concerning –

(a) the establishment of a high common level of security of network and information systems;

(b) the adoption of a national strategy on the security of network and information systems;

(c) a European Cooperation Group;

(d) a CSIRTs network;

(e) security and notification requirements for operators of essential services and for digital service providers; and

(f) obligations of national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

(2) This Part does not apply to –

(a) undertakings which are subject to the requirements of Articles 13a and 13b of the Framework Directive;

(b) trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.

(3) This Part applies without limiting –

(a) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;

(b) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA; and

(c) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

(4) The Competent Authority may share information with the Gibraltar CSIRT, the European Commission and relevant authorities in other Member States if that information sharing is –

(a) necessary for the application or requirements of this Part;

(b) the information exchanged is limited to that which is relevant and proportionate to the purpose of such sharing of information; and

(c) such information sharing preserves the confidentiality of that information and protects the security and commercial interests of operators of essential services and digital service providers.

(5) Nothing in this Part limits the taking of any action (or the lack of any action) which any person may consider necessary for the purposes of safeguarding essential Government or State functions in Gibraltar, in particular –

(a) safeguarding national security, including actions protecting information the disclosure of which the person considers is contrary to the essential interests of the security of Gibraltar; and

(b) maintaining law and order in Gibraltar, in particular to allow for the investigation, detection and prosecution of criminal offences.

(6) Where an operator of essential services or digital service provider is required either to ensure the security of their network and information systems or to notify incidents pursuant to:

(a) a sector-specific European Union law; or

(b) any statutory provision under Gibraltar law giving effect to a sector-specific European Union law,

then the provisions of that sector-specific European Union or Gibraltar law shall apply, subject to such requirements being at least equivalent in effect to the obligations laid down in this Part.

Data protection.

33. The processing of personal data under this Part shall be carried out in accordance with the Data Protection Act 2004 and Regulation (EC) No 45/2001.

Interpretation.

34. In this Part–

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

"CSIRTs network" means the network of national computer security incident response teams ('CSIRTs') established under Article 12(1) of the NIS Directive;

"Data Protection Commissioner" means the Data Protection Commissioner within the meaning of section 21 of the Data Protection Act 2004;

"digital service" means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services which is of a type listed in Schedule 5;

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

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

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

"European Commission" means the Commission of the European Union;

"European Cooperation Group" means the Cooperation Group established under Article 11(1) of the NIS Directive;

"Framework Directive" means Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, as amended by Directive 2009/140/EC of the

European Parliament and of the Council of 25 November 2009, as amended from time to time;

"Gibraltar Regulatory Authority" means the body established under section 3(1) of the Gibraltar Regulatory Authority Act 2000;

"incident" means any event having an actual adverse 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 (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;

"Member State" means a Member State of the European Union;

"the Minister" means the Minister with responsibility for Commerce;

"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

(a) an electronic communications network within the meaning of point (a) of Article 2 of the Framework Directive;

(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 points (a) and (b) above for the purposes of their operation, use, protection and maintenance;

"NIS Directive" means 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 European Union;

"online marketplace" means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) to conclude online sales or service 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 any person designated as an operator of essential services under section 35(2);

"risk" means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

"representative" means any natural or legal person established in the European Union explicitly designated to act on behalf of a digital service provider not established in the European 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 Part;

"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 point (1) of Article 2 of Regulation (EU) No 1025/2012;

"specification" means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;

"top-level domain name registry" means an entity which administers and operates the registration of internet domain names under a specific top-level domain ('TLD').

Identification and designation of operators of essential services.

35.(1) The Competent Authority must, by 9th November 2018, for each sector and subsector referred to in Schedule 4, identify operators of essential services established in Gibraltar.

(2) The Competent Authority may designate a person as an operator of essential services if it provides a service of a kind specified in Schedule 4, and the following conditions are met—

(a) that person provides a service which is essential for the maintenance of critical societal or economic activities (an "essential service");

(b) the provision of that essential service by that person relies on network and information systems; and

(c) in the opinion of the Competent Authority an incident affecting the provision of that essential service by that person is likely to have significant disruptive effects on the provision of that essential service.

(3) In order to arrive at the conclusion mentioned in subsection (2)(c), the Competent Authority must have regard to the following factors—

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

(b) the degree of dependency of the other relevant sectors on the service provided by that person;

(c) the likely impact of incidents on the essential service provided by that person, in terms of its degree and duration, on economic and societal activities or public safety;

(d) the market share of the essential service provided by that person;

(e) the geographical area that may be affected if an incident impacts on the service provided by that person;

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

(g) any other factor the Competent Authority considers appropriate to have regard to.

(4) The Competent Authority must designate an operator of essential services under subsection (2) by notice in writing served on the person who is to be designated and provide reasons for the designation in the notice.

(5) Before the Competent Authority designates a person as an operator of essential services under subsection (2), the Competent Authority may—

(a) request information from that person under section 48(1); and

(b) invite the person to submit any written representations about the proposed decision to designate it as an operator of essential services.

(6) The Competent Authority must consult with the relevant authorities in another Member State before designating a person as an operator of essential services under subsection (2) if that person already provides an essential service in that Member State.

(7) The Competent Authority must maintain a list of all persons designated as operators of essential services under subsection (2).

(8) The Competent Authority must review the list mentioned in subsection (7) at regular intervals and in accordance with subsection (9).

(9) The first review under subsection (8) must take place before 9th May 2020, and subsequent reviews must take place, at least, biennially.

(10) The Minister may make regulations under section 55 to make provision for a person to be deemed to be designated as an operator of essential services against such criteria or thresholds as the Minister may in such regulations provide.

(11) The Competent Authority must establish a list of essential services as mentioned in subsection (2)(a).

(12) The Competent Authority must, on or before 9th November 2018, and on a biennial basis thereafter, submit to the European Commission the information necessary to enable the European Commission to assess the implementation of the NIS Directive under Gibraltar law.

(13) The information mentioned in subsection (12) must include information on –

(a) national measures allowing for the identification of operators of essential services;

(b) the list of essential services;

(c) the number of operators of essential services identified for each sector referred to in Schedule 4 and an indication of their importance in relation to that sector;

(d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in subsection 3(a) or to the importance of that particular operator of essential services as referred to in subsection 3(f).

Revocation of designation.

36.(1) The Competent Authority may revoke a designation of a person under section 35(2) if it is of the opinion that the conditions mentioned in that section are no longer met by that person.

(2) Before revoking a designation of a person under section 36(1), the Competent Authority must—

(a) serve a notice in writing of the proposed revocation on that person;

(b) provide reasons for the proposed decision;

(c) invite that person to submit any written representations about the proposed decision within such time period as may be specified by the Competent Authority; and

(d) consider any representations submitted by the person under subsection 2(c) before a final decision is taken to revoke the designation.

(3) In order to arrive at the conclusion mentioned in subsection (1), the Competent Authority must have regard to the factors mentioned in section 35(3).

(4) The Competent Authority may revoke a designation of a person under section 36(1), if the Competent Authority has received a request from another Member State to do so and the Competent Authority is in agreement that the designation of that person should be revoked.

National strategy on the security of network and information systems.

37.(1) The Minister must adopt a national strategy to provide appropriate policy, priorities, regulatory measures and strategic objectives on the security of network and information systems in Gibraltar (the "Gibraltar NIS strategy").

(2) The objectives, measures and priorities set out in the Gibraltar NIS strategy must be aimed at achieving and maintaining a high level of security of network and information systems in Gibraltar in –

(a) the sectors referred to in Schedule 4 and;

(b) the services referred to in Schedule 5.

(3) The Gibraltar NIS strategy may be –

(a) published in such form and manner as the Minister considers appropriate; and

(b) updated by the Minister at any time.

(4) The Gibraltar NIS strategy must 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 strategy.

(5) The Minister may request the assistance of the European Union Agency for Network and Information Security ('ENISA'), in developing the Gibraltar NIS strategy.

(6) The Minister must communicate the Gibraltar NIS strategy, including any updated versions, to the European Commission within three months of the date of adoption.

(7) Before communicating the Gibraltar NIS strategy to the European Commission, the Minister may redact any elements which relate to national security.

Designation of national competent authority and single point of contact.

38.(1) The Gibraltar Regulatory Authority is designated as the competent authority in Gibraltar on the security of network and information systems in respect of the sectors referred to in Schedule 4 and services referred to in Schedule 5 (the "**Competent Authority"**).

(2) The Competent Authority is, for the purposes of and in accordance with the procedures under this Part, responsible for –

(a) regulating, supervising and enforcing compliance with the conditions and, where applicable, the specific obligations, to which an operator of essential services or a digital service provider may be subject;

(b) without limiting subsection (2), investigating any breach of any one or more of the following–

(i) this Part;

(ii) any regulations, Codes of Practice or Guidance Notes made under this Part;

(iii) any condition and, where applicable, specific obligation imposed on a person,

(c) keeping under review the operation and application of this Part; and

(d) preparing and publishing guidance for operators of essential services or digital service providers.

(3) Any guidance that is published by the Competent Authority under this Part may be–

(a) published in such form and manner as the Competent Authority considers appropriate; and

(b) reviewed at any time by the by the Competent Authority.

(4) The Competent Authority is designated as the single point of contact on the security of network and information systems for Gibraltar.

(5) In order to ensure cross border co-operation and fulfil the requirements of this Part, the Competent Authority must liaise with –

(a) the relevant authorities in other Member States;

(b) the European Cooperation Group; and

(c) the CSIRTs network.

(6) The Minister must ensure that the Competent Authority has access to adequate resources with which to –

(a) effectively and efficiently carry out the tasks assigned to it; and

(b) ensure compliance with this Part.

(7) The Minister must ensure the effective, efficient and secure cooperation of Gibraltar's designated representative in the European Cooperation Group.

(8) The Competent Authority must, as it considers appropriate, consult and cooperate with Gibraltar law enforcement authorities in performing the functions assigned to it under this Part.

(9) The Competent Authority must, as it considers appropriate, consult and cooperate with the Data Protection Commissioner and any other relevant data protection authorities when addressing incidents resulting in personal data breaches.

(10) The Minister must without delay and in accordance with Article 8(7) of the NIS Directive, notify the European Commission of –

(a) the designation of the Competent Authority;

(b) the designation of the single point of contact;

(c) the Competent Authority's tasks; and

(d) any subsequent change thereto.

Designation of computer security incident response team (CSIRT).

39.(1) The Information, Technology & Logistics Department is designated as the national computer security incident response team for Gibraltar (the "Gibraltar CSIRT").

(2) The Gibraltar CSIRT must comply with the requirements and tasks set out in Schedule 3 covering at least the sectors referred to in Schedule 4 and the services referred to in Schedule 5.

(3) The Minister must ensure that –

(a) the Gibraltar CSIRT has access to adequate resources with which to effectively carry out its tasks as set out in Schedule 3;

(b) the Gibraltar CSIRT has access to adequate resources with which to cooperate in an effective, efficient and secure manner with other CSIRTs in the CSIRTs network;

(c) the Gibraltar CSIRT has access to an appropriate, secure, and resilient communication and information infrastructure;

(d) the European Commission is informed of the remit and main elements of the incident handling process of the Gibraltar CSIRT.

(4) The Minister may request the assistance of ENISA in developing the Gibraltar CSIRT.

Cooperation at national level.

40.(1) The Competent Authority and the Gibraltar CSIRT must cooperate with regards to the fulfilment of the obligations laid down in this Part.

(2) The Competent Authority must, to the extent necessary for the Gibraltar CSIRT to fulfil its tasks, grant the Gibraltar CSIRT access to data on incidents notified to the Competent Authority –

(a) by operators of essential services pursuant to section 42; or

(b) by digital service providers pursuant to section 43.

(3) The Competent Authority must, on or before 9th August 2018, and on an annual basis thereafter, submit to the European Cooperation Group a summary report on the incident notifications received, including –

(a) the number of notifications received;

(b) the nature of the incidents notified;

(c) the actions taken in relation to notifications received under section 42(1);

(d) the actions taken in accordance with section 42(5);

(e) the actions taken in accordance with section 42(6)(a);

(f) the actions taken in relation to notifications received under section 43(3); and

(g) the actions taken in accordance with section 43(9).

Operators of essential services - security requirements.

41.(1) An operator of essential services must 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.

(2) An operator of essential services must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

(3) The measures taken by an operator of essential services under subsection (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.

(4) Operators of essential services must have regard to any relevant guidance issued by the Competent Authority when carrying out the duties imposed by subsections (1) and (2).

Operators of essential services - incident notification

42.(1) An operator of essential services must notify the Competent Authority of any incident having a significant impact on the continuity of the essential service which that operator of essential services provides ("NIS incident").

(2) The notification in subsection (1) must –

(a) provide the following—

(i) the operator's name and the essential services it provides;

(ii) the time the NIS incident occurred;

(iii) the duration of the NIS incident;

(iv) information concerning the nature and impact of the NIS incident;

(v) information concerning any, or any likely, cross-border impact of the NIS incident;

(vi) any other information that may be helpful to the Competent Authority; and

(b) be provided to the Competent Authority —

(i) without undue delay as soon as the operator of essential services is aware that a NIS incident has occurred; and

(ii) in such form and manner as the Competent Authority determines.

(3) The notification in subsection (1) does not make the notifying party subject to increased liability.

(4) In order to determine the significance of the impact of an incident, an operator of essential services must have regard to the following factors –

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

(b) the duration of the incident; and

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

(5) On the basis of information provided in a notification under subsection (1), the Competent Authority must inform any other affected Member States

if the incident has a significant impact on the continuity of essential services in that Member State.

(6) Following receipt of a notification under subsection (1), the Competent Authority may inform—

(a) the operator of essential services who provided the notification about any relevant information that relates to the NIS incident, including how it has been followed up, in order to assist that operator of essential services to deal with that incident more effectively or prevent a future incident; and

(b) the public about the NIS incident, as soon as reasonably practicable, if the Competent Authority is of the view that public awareness is necessary in order to handle that incident or prevent a future incident.

(7) Prior to the Competent Authority informing the public about a NIS incident under subsection 6(b), the Competent Authority must first consult the operator of essential services who provided the notification under subsection (1).

(8) The Competent Authority is not required to share information with other Member States under subsection (5) if the information is—

(a) confidential; or

(b) the information sharing may prejudice the security or commercial interests of an operator of essential services.

Digital service providers - security requirements and incident notification.

43.(1) A digital service provider must 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 the services referred to in Schedule 5 within the European Union.

(2) The measures taken by a digital service provider under subsection (1) must –

(a) having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed;

(b) prevent and minimise the impact of incidents affecting the security of their network and information systems with a view to ensuring the continuity of those services; and

(c) take into account the following elements:

(i) the security of systems and facilities;

(ii) incident handling;

(iii) business continuity management;

(vi) monitoring, auditing and testing;

(v) compliance with international standards.

(3) A digital service provider must, without undue delay, notify the Competent Authority of any incident having a substantial impact on the provision of any service as mentioned in subsection (1) that it provides ("Substantial incident").

(4) The notification mentioned under subsection (3) must include sufficient information to enable the Competent Authority to determine the significance of any cross-border impact and provide the following–

(a) the digital service provider's name and the services it provides;

(b) the time the Substantial incident occurred;

(c) the duration of the Substantial incident;

(d) information concerning the nature and impact of the Substantial incident;

(e) information concerning any, or any likely, cross-border impact of the Substantial incident; and

(f) any other information that may be helpful to the Competent Authority.

(5) The notification mentioned in subsection (3) does not make the notifying party subject to increased liability.

(6) In order to determine whether the impact of an incident is substantial for the purposes of subsection (3), 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.

(7) The obligation to notify an incident under subsection (3) applies subject to the digital service provider having access to the information needed to assess the impact of an incident against the parameters referred to in subsection (6).

(8) If an operator of essential services relies on a third-party digital service provider for the provision of an essential service, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified to the Competent Authority by that operator of essential services.

(9) If an incident notified under subsection (3) affects two or more Member States, the Competent Authority must inform the relevant authorities in each of the affected Member States about that incident.

(10) The Competent Authority is not required to share information under subsection (9) if the information contains—

(a) confidential information; or

(b) information which may prejudice the security or commercial interests of a digital service provider.

(11) If the Competent Authority—

(a) consults with the digital service provider responsible for an incident notification under subsection (3); and

(b) is of the view that public awareness about that incident is necessary to prevent or manage it, or is in the public interest,

the Competent Authority may, subject to subsection (12), inform the public about that incident or direct the digital service provider responsible for the notification to do so.

(12) Before the Competent Authority informs the public about an incident notified under subsection (3), the Competent Authority must consult the digital service provider who provided the notification.

(13) This Part applies subject to any delegated acts adopted by the European Commission under Article 16(8) or Article 16(9) of the NIS Directive.

(14) Sections 43, 44, 48(3), 49(2), 49(3) and 50(2) shall not apply to micro and small enterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium–sized enterprises.

(15) Where –

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

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

the Competent Authority must cooperate with and assist the competent authorities of those other Member States as necessary.

(16) The cooperation and assistance referred to in subsection (15) may cover –

(a) information exchanges between the Competent Authority and the competent authorities of other Member States concerned; and

(b) requests to take the measures referred to in sections 43, 44, 48(3), 49(2), 49(3) and 50(2).

Jurisdiction and territoriality of digital service providers

44.(1) For the purposes of this Part–

(a) a digital service provider shall be deemed to be under the jurisdiction of Gibraltar if it has its main establishment in Gibraltar;

(b) a digital service provider shall be deemed to have its main establishment in Gibraltar when it has its head office in Gibraltar.

(2) A digital service provider that is not established within the European Union but offers services referred to in Schedule 5 within the European Union, shall be deemed to be under the jurisdiction of Gibraltar where its representative is established in Gibraltar.

Standardisation.

45.(1) The Minister must, when making any regulations under section 55 with respect to any matters mentioned in section 41 or 43, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems without imposing, or discriminating in favour of the use of, a particular type of technology.

(2) The Competent Authority must, when drawing up or issuing any Codes of Practice or Guidance Notes under section 54 with respect to any matters mentioned in section 41 or 43, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems without imposing, or discriminating in favour of the use of, a particular type of technology.

Voluntary notification.

46.(1) Entities which have not been designated under section 35(2) as operators of essential services and are not digital service providers may on a voluntary basis notify the Competent Authority of incidents having a significant impact on the continuity of the services which they provide.

(2) Any notifications made under subsection (1) must be processed by the Competent Authority in the same manner and in accordance with the same procedure as mandatory notifications made under this Part.

(3) The Competent Authority may prioritise the processing of mandatory notifications made under this Part over voluntary notifications.

(4) Voluntary notifications must only be processed where such processing would not constitute a disproportionate or undue burden on the Competent Authority.

(5) A notifying entity which makes a voluntary notification shall not have any obligations imposed upon it to which it would not have been subject had it not made such notification.

Implementation and enforcement.

47.(1) The Competent Authority shall have a duty to perform the functions assigned to it under this Part.

(2) Subject to the provisions of this Part, and to this or any other Act, the Competent Authority may do anything that appears to it to be incidental or conducive to the carrying out of its duties under this Part.

Information notices.

48.(1) In order to assess whether a person is an operator of essential services for the purposes of section 35, the Competent Authority may serve an information notice upon any person requiring that person to provide it with any information that it may reasonably require to establish whether that or any other person is an operator of essential services.

(2) The Competent Authority may serve an information notice upon an operator of essential services requiring that person to provide it with information that it reasonably requires to assess—

(a) the security of its network and information systems, including its documented security policies;

(b) the operator of essential services' compliance with section 41;

(c) the implementation of its security policies, including information about inspections conducted under section 49 and any underlying evidence in relation to such an inspection.

(3) The Competent Authority may serve upon a digital service provider an information notice requiring it to provide the Competent Authority with information that the Competent Authority reasonably requires to assess—

(a) the security of the digital service provider's network and information systems, including its documented security policies;

(b) the digital service provider's compliance with section 43; and

(c) the implementation of its security policies, including any about inspections conducted under section 49 and any underlying evidence in relation to such an inspection.

(4) An information notice must—

(a) describe the information that is required by the Competent Authority;

(b) provide the reasons for requesting such information;

(c) specify the form and manner in which the requested information is to be provided; and

(d) specify the time period within which the information must be provided.

(5) In a case falling within subsection (1) the information notice may—

(a) be served by publishing it in such manner as the Competent Authority considers appropriate in order to bring it to the attention of any persons who are described in the notice as the persons from whom the information is required; and

(b) take the form of a general request for a certain category of persons to provide the information that is specified in the notice.

(6) The Competent Authority may withdraw an information notice by written notice to the person on whom it was served.

Power of inspection.

49.(1) The Competent Authority in relation to an operator of essential services may—

(a) conduct an inspection;

(b) appoint a person to conduct an inspection on its behalf; or

(c) direct the operator of essential services to appoint a person who is approved by the Competent Authority to conduct an inspection on its behalf,

to assess if the operator of essential services has fulfilled the duties imposed on it by section 41.

(2) The Competent Authority may—

(a) conduct an inspection;

(b) appoint a person to conduct an inspection on its behalf; or

(c) direct that a digital service provider appoint a person who is approved by the Competent Authority to conduct an inspection on its behalf,

to assess if a digital service provider has fulfilled the requirements set out in section 43.

(3) For the purposes of carrying out the inspection under subsection (1) or (2), the operator of essential services or digital service provider (as the case may be) must—

(a) pay the reasonable costs of the inspection;

(b) co-operate with the person who is conducting the inspection ("the inspector");

(c) provide the inspector with reasonable access to their premises;

(d) allow the inspector to inspect, copy or remove such documents and information, including information that is held electronically, as the inspector considers to be relevant to the inspection; and

(e) allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection.

(4) The Competent Authority may appoint a person to carry out an inspection under subsections (1)(b) or (2)(b) on its behalf on such terms and in such a manner as it considers appropriate.

Enforcement for breach of duties.

50.(1) The Competent Authority may serve an enforcement notice upon an operator of essential services if the Competent Authority has reasonable grounds to believe that the operator of essential services has failed to—

(a) fulfil the security duties under section 41;

(b) notify an incident under section 42;

(c) notify an incident as required by section 43(8);

(d) comply with an information notice issued under section 48 or

(e) comply with—

(i) a direction given under section 49(1)(c), or
(ii) the requirements stipulated in section 49(3).

(2) The Competent Authority may serve an enforcement notice upon a digital service provider if the Competent Authority has reasonable grounds to believe that the digital service provider has failed to—

(a) fulfil its duties or notify an incident under section 43;

(b) comply with a direction made by the Competent Authority under section 43(11);

(c) comply with an information notice issued under section 48; or

(d) comply with—

(i) a direction given under section 49(2)(c), or
(ii) the requirements stipulated in section 49(3).

(3) An enforcement notice that is served under subsection (1) or (2) must be in writing and must specify the following—

(a) the reasons for serving the notice;

(b) the alleged failure which is the subject of the notice;

(c) what steps, if any, must be taken to rectify the alleged failure and the time period during which such steps must be taken; and

(d) how and when representations may be made about the content of the notice and any related matters.

(4) If the Competent Authority is satisfied that no further action is required, having considered—

(a) the representations submitted in accordance with subsection (3)(d); or

(b) any steps taken to rectify the alleged failure;

it must inform the operator of essential services or the digital service provider, as the case may be, in writing, as soon as reasonably practicable.

Penalties.

51.(1) The Competent Authority may serve a penalty notice upon an operator of essential services if the operator of essential services was served

with an enforcement notice under section 50(1) and the operator of essential services —

(a) was required to take steps to rectify a failure within a time period stipulated in the enforcement notice but the operator failed to take any steps or any adequate steps; or

(b) was not required to take steps to rectify a failure but the Competent Authority is not satisfied with the representations submitted by the operator of essential services in accordance with section 50(3)(d).

(2) The Competent Authority may serve a penalty notice upon a digital service provider if the digital service provider was served with an enforcement notice under section 50(2) and the digital service provider —

(a) was required to take steps to rectify a failure within a time period stipulated in the enforcement notice but the digital service provider failed to take any steps or any adequate steps; or

(b) was not required to take steps to rectify a failure but the Competent Authority is not satisfied with the representations submitted by the digital service provider in accordance with section 50(3)(d).

(3) A penalty notice must be in writing and must specify the following—

(a) the reasons for imposing a penalty;

(b) the sum that is to be imposed as a penalty and how it is to be paid;

(c) the date on which the notice is given;

(d) the date, at least 30 days after the date specified in subsection (c), before which the penalty must be paid ("the payment period");

(e) details about the independent review process under section 52 and how the right to review may be exercised; and

(f) the consequences of failing to make payment within the payment period.

(4) The Competent Authority may withdraw a penalty notice by informing the person upon whom it was served in writing.

(5) The sum that is to be imposed under a penalty notice served under this section must be an amount that—

(a) the Competent Authority determines is appropriate and proportionate to the failure in respect of which it is imposed; and

(b) is in accordance with subsection (6).

(6) The amount that is to be imposed under a penalty notice must—

(a) not exceed £25,000 for any contravention which the Competent Authority determines could not cause an incident;

(b) not exceed the higher of £1,000,000 or 1% of annual turnover for a material contravention which the Competent Authority determines has caused, or could cause, an incident resulting in a reduction of service provision by the operator of essential services or digital service provider for a significant period of time;

(c) not exceed the higher of £2,000,000 or 2% of annual turnover for a material contravention which the Competent Authority determines has caused, or could cause, an incident resulting in a disruption of service provision by the operator of essential services or digital service provider for a significant period of time;

(d) not exceed the higher of £5,000,000 or 5% of annual turnover for a material contravention which the Competent Authority determines has caused, or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the Gibraltar economy.

(7) In this section –

(a) "annual turnover" means the total annual turnover according to the last available accounts approved by the management body of the provider of essential services or the digital service provider, as the case may be;

(b) "a material contravention" means a failure to take steps, or any adequate steps, within the stipulated time period to rectify a failing that is described in section 50(1)(a) to (d) or section 50(2)(a) to (c).

Independent review of designation decisions and penalty decisions.

52.(1) If an operator of essential services so requests, the Competent Authority must appoint an independent person ("the reviewer") to conduct reviews of a designation or penalty decision made by the Competent Authority in relation to that operator of essential services.

(2) The Competent Authority must appoint an independent person ("the reviewer") to conduct a review of a penalty decision made by the Competent Authority in relation to a digital service provider, if the digital service provider requests a review to be conducted.

(3) An operator of essential services may request the reviewer to review a designation or penalty decision made in relation to that operator of essential services in order to challenge any of the following matters—

(a) the basis upon which the designation decision was made;

(b) the grounds for imposing a penalty notice;

(c) the sum that is imposed by way of a penalty notice;

(d) the time period within which the penalty notice must be paid.

(4) A digital service provider may request the reviewer to conduct a review of a penalty decision made in relation to that digital service provider in order to challenge any of the following matters—

(a) the grounds for imposing a penalty notice;

(b) the sum that is imposed by way of a penalty notice;

(c) the time period within which the penalty notice must be paid.

(5) Any request to conduct a review must—

(a) be made in writing to the Competent Authority;

(b) set out the reasons for requesting a review and provide any relevant evidence; and

(c) be made within 30 days of receipt of the designation decision or penalty decision.

(6) The Competent Authority must respond to a request, including to any reasons provided under section 52(5)(b), to conduct a review—

(a) in writing to the reviewer, copied to the person who made the request for a review; and

(b) within 30 days of receipt of that request.

(7) The reviewer may extend the time limits mentioned in subsection (5)(c) or (6)(b) if the reviewer considers it necessary to do so in the interests of fairness and having regard to the facts and circumstances of the particular case.

(8) A request for a review suspends the effect of a designation decision or penalty decision until the review is decided or withdrawn.

(9) The reviewer must uphold or set aside a designation decision or a penalty decision after consideration of the following matters—

(a) the basis upon which the designation decision or penalty decision is challenged;

(b) the response submitted under subsection (6); and

(c) any relevant evidence.

(10) The reviewer must provide reasons for the decision made under subsection (9).

(11) In this section—

(a) "designation decision" means a decision to designate an operator of essential services made by way of notice under section 35(2); and

(b) "penalty decision" means a decision to serve a penalty notice under section 51(1) or (2).

Enforcement of penalty notices.

53.(1) This section applies where a sum is payable to the Competent Authority as a penalty under section 51.

(2) A penalty imposed under this Part may be enforced as if it was a civil debt owed to the Competent Authority.

Codes of Practice and Guidance Notes.

54.(1) The Competent Authority may, in such manner and by such means as it considers most effective, promote the following of good practice by operators of essential services and digital service providers so as to promote compliance with this Part, including through–

(a) drawing up codes of practice as to good practice in relation to the discharge by an operator of essential services or a digital service provider of its duties under any of the provisions of this Part ("Codes of Practice");

(b) issuing guidance consisting of such information and advice as it considers appropriate ("Guidance Notes") –

(i) with respect to matters within its competence relating to the operation of this Part;

(ii) with respect to any matters relating to the discharge by the Competent Authority of its functions under this Part;

(iii) with respect to any other matters within the statutory competence of the Competent Authority about which it appears to the Competent Authority to be desirable to give information or advice.

Regulations.

55.(1) The Minister may make regulations for the purpose of bringing any part of this Part or the NIS Directive into effect and for any matters for which provisions are made in this Part.

(2) The Minister may make regulations empowering the Competent Authority to prescribe by rules anything for which provision may be made under this Part or the NIS Directive.

(3) Without limiting the generality of subsections (1) or (2), or any other express provision of this Part, regulations made by the Minister may–

(a) contain such transitional provisions, and such incidental or supplementary provisions, as appear to the Minister to be expedient for the purposes of this Part;

(b) make different provisions in relation to different cases, circumstances or operators of essential services or digital service providers;

(c) apply to all essential services and digital services or to any category or description of essential services or digital services or services which are essential for the maintenance of critical societal or economic activities;

(d) exempt any person from any of the provisions of this Part;

(e) set out general conditions applicable to all operators of essential services or digital service providers covered by this Part or to prescribed classes of operators of essential services or digital service providers;

(f) make different provisions in respect of the different cases mentioned in subsections (b) and (c) and in respect of different circumstances within those cases.

(4) Any power conferred by this Part to make regulations includes a power to vary or revoke any regulation so made by a subsequent regulation.

(5) Regulations and rules made by the exercise of powers contained in this section shall be laid before the Parliament in accordance with the provisions of section 28 of the Interpretation and General Clauses Act but shall not require the prior approval of the Parliament before coming into force.".

Insertion of Schedule 3.

4. The following is inserted after Schedule 2 -

"SCHEDULE 3

Section 39

REQUIREMENTS AND TASKS OF THE GIBRALTAR COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT)

The Gibraltar CSIRT –

(1) Must ensure a high level of availability of its communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times.

(2) Must ensure its communication channels are clearly specified and well known to the constituency and cooperative partners.

(3) Must ensure that its premises and supporting information systems are located in secure sites.

(4) Must, in respect of business continuity:

(a) be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers;

(b) be adequately staffed to ensure availability at all times;

(c) only rely on an infrastructure the continuity of which is ensured, including the availability of redundant systems and backup working space.

(5) May participate in international cooperation networks.

(6) Must:

(a) monitor incidents in Gibraltar;

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

(c) respond to any incidents;

(d) provide dynamic risk and incident analysis and situational awareness;

(e) participate and cooperate in the CSIRTs network.

(8) Must establish cooperation relationships with the private sector.

(9) Must facilitate cooperation by promoting the adoption and use of common or standardised practices for –

(a) incident and risk-handling procedures;

(b) incident, risk and information classification schemes.".

Insertion of Schedule 4.

5. The following is inserted after Schedule 3 -

"SCHEDULE 4

Section 34

TYPES OF ENTITIES FOR THE PURPOSES OF THE INTERPRETATION OF "OPERATORS OF ESSENTIAL SERVICES" UNDER PART 7

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 Section 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 who 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

(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 counter- parties 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).".

Insertion of Schedule 5.

6. The following is inserted after Schedule 4 -

"SCHEDULE 5

Section 34

TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF THE INTERPRETATION OF "DIGITAL SERVICE" UNDER PART 7

1. Online marketplace
2. Online search engine
3. Cloud computing service"

Dated 8th May, 2018.

A J ISOLA,
Minister with responsibility for Commerce.

EXPLANATORY MEMORANDUM

These Regulations add a new Part 7 to the Civil Contingencies Act 2007 and add new Schedules 3, 4 and 5 to that Act in order to transpose 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 European Union.

Printed by the Gibraltar Chronicle Printing Limited
Unit 3, New Harbours
Government Printers for Gibraltar,
Copies may be purchased at 6, Convent Place, Price £2.75