Civil Contingencies Act 2007

Principal Act

Act. No. 2007-14 *Commencement* 26.4.2007
Assent 20.4.2007

Amending enactments	Relevant current provisions	Commencement date
LN. 2011/064	ss. 21-30, Sch. 1-2	12.5.2011
2013/012	s. 31	31.1.2013
2018/102	ss. 32-55, Sch. 3-5	10.5.2018
2018/124	s. 34	25.5.2018
Act. 2017-10	s. 18(2)	13.6.2018
2018-12	ss. 34, 38(9)	1.6.2021
LN. 2024/087	ss. 32(1)(c), (2)(a), (3)(a)-(c), (4), (6), 33-34, 35(6), (12)-(13), 36(4), 37(5)-(7), 38(5), (a), (7), (10), 39(3)(b), (d), (4), 40(3), 42(5), (8), 43(1), (6A), (9)-(10), (13), (15)-(16), 44(2), 55(1)-(2), Sch. 3	23.5.2024
2025/032	Sch. 1	24.1.2025

Transposing:
Directive 2008/114/EC
Directive (EU) 2016/1148

Implementing:
Regulation (EU) 2016/679

ARRANGEMENT OF SECTIONS

Section

SCHEDULE 3
REQUIREMENTS AND TASKS OF THE GIBRALTAR COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT)

SCHEDULE 4
TYPES OF ENTITIES FOR THE PURPOSES OF THE INTERPRETATION OF "OPERATORS OF ESSENTIAL SERVICES" UNDER PART 7

SCHEDULE 5
TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF THE INTERPRETATION OF "DIGITAL SERVICE" UNDER PART 7

AN ACT TO MAKE PROVISION FOR THE EXERCISE OF CERTAIN POWERS IN THE EVENT OF, IN THE CONTEXT OF, AND IN RELATION TO, CIVIL CONTINGENCIES.

PART 1
General

Title and commencement.

1. This Act may be cited as the Civil Contingencies Act 2007 and comes into operation on the day of publication.

Interpretation.

2. In this Act–

"emergency" has the meaning given by section 10;

"function" means any power or duty whether conferred by virtue of an enactment or otherwise;

"Minister" means the Minister for Civil Contingencies, acting with the consent of the Chief Minister;

"public functions" means–

(a) functions conferred or imposed by or by virtue of an enactment,

(b) functions of Ministers (or their departments),

(c) functions of public officers;

"serious delay" means a delay that might–

(a) cause serious damage; or

(b) obstruct the prevention, control or mitigation of serious damage.

PART 2
Pre-emptive measures

Pre-emptive measures.

3.(1) Where the Government believes that an event or situation threatens damage to human welfare in Gibraltar it may make regulations to prevent, mitigate or control the effects of that event or situation.

(2) An event or situation threatens damage to human welfare only if, on a scale which is greater than the normal risk or incidence thereof, it involves, causes or may cause–

(a) loss of human life;

(b) human illness or injury;

(c) homelessness;

(d) damage to property;

(e) disruption of a supply of money, food, water, energy or fuel;

(f) disruption of a system of communication;

(g) disruption of facilities for transport; or

(h) disruption of services relating to health.

(3) The event or situation mentioned in subsection (1) may occur or be inside or outside Gibraltar.

(4) Regulations made under subsection (1) may impose penalties of a maximum of 5 years imprisonment and fines not exceeding £20,000, and subject to the provisions of the Constitution may provide for the confiscation of goods.

General measures.

4.(1) The Minister may by order require a person or body listed in the Schedule 1 to perform a function of that person or body for the purpose of–

(a) preventing the occurrence of an emergency;

(b) reducing, controlling or mitigating the effects of an emergency; or

(c) taking other action in connection with an emergency.

(2) A person or body shall comply with an order under this section.

(3) An order under subsection (1) may–

(a) require a person or body to consult a specified person or body or class of person or body;

(b) permit, require or prohibit collaboration, to such extent and in such manner as may be specified;

(c) permit, require or prohibit delegation, to such extent and in such manner as may be specified;

(d) permit or require a person or body listed in the Schedule 1 to co-operate, to such extent and in such manner as may be specified, with another person or body listed in the Schedule 1 in connection with a duty under the order;

(e) permit or require a person or body listed in the Schedule 1 to provide information in connection with a duty under the order, whether on request or in other specific circumstances to a person or body listed in the Schedule 1;

(f) confer a function on a Minister or on any other specified person or body (and a function conferred may, in particular, be a power or duty to exercise a discretion);

(g) make provision which applies generally or only to a specified person or body or only in specified circumstances;

(h) make different provision for different persons or bodies or for different circumstances.

Urgency.

5.(1) This section applies where–

(a) there is an urgent need to make provision of a kind that could be made by an order under section 4(1); but

(b) there is insufficient time for the order to be made.

(2) The Chief Minister may by direction make provision of a kind that could be made by an order under section 4(1).

(3) A direction under subsection (2) shall be in writing.

(4) Where the Chief Minister gives a direction under subsection (2)–

(a) he may revoke or vary the direction by further direction,

(b) he shall revoke the direction as soon as is reasonably practicable (and he may, if or in so far as he thinks it desirable, re-enact the substance of the direction by way of an order under section 4(1)), and

(c) the direction shall cease to have effect at the end of the period of 21 days beginning with the day on which it is given (but without prejudice to the power to give a new direction).

(5) A provision of a direction under subsection (2) shall be treated for all purposes as if it were a provision of an order under section 4(1).

Monitoring by Government.

6.(1) A Minister may require a person or body listed in the Schedule 1–

(a) to provide information about action taken by the person or body for the purpose of complying with a duty under this Part, or

(b) to explain why the person or body has not taken action for the purpose of complying with a duty under this Part.

(2) A requirement under subsection (1) may specify–

(a) a period within which the information or explanation is to be provided;

(b) the form in which the information or explanation is to be provided.

(3) A person or body shall comply with a requirement under subsection (1).

Enforcement.

7.(1) Any of the following may bring proceedings in the Supreme Court in respect of a failure by a person or body listed in the Schedule 1 to comply with section 4(2) or 6(3)–

(a) the Minister;

(b) a person or body listed in the Schedule 1.

(2) In proceedings under subsection (1) the Supreme Court may grant any relief, or make any order, that it thinks appropriate.

Provision of information.

8. Regulations or an order under this Part may, if addressing the provision or disclosure of information, make provision about

(a) timing;

(b) the form in which information is provided;

(c) the use to which information may be put;

(d) storage of information;

(e) disposal of information.

Amendment of Schedule 1.

9.(1) The Chief Minister may by order amend the Schedule 1.

(2) An order under subsection (1)–

(a) may add, remove or move an entry either generally or only in relation to specified functions of a person or body, and

(b) may make incidental, transitional or consequential provision (which may include provision amending this or another enactment).

PART 3
Emergency

Meaning of "emergency".

10.(1) In this Act "emergency" means–

(a) an event or situation which threatens serious damage to human welfare in Gibraltar; or

(b) an event or situation which threatens serious damage to the environment of Gibraltar.

(2) For the purposes of subsection (1)(a) an event or situation threatens damage to human welfare only if, on a scale which is greater that the normal risk or incidence thereof, it involves, causes or may cause–

(a) loss of human life;

(b) human illness or injury;

(c) homelessness;

(d) damage to property;

(e) disruption of a supply of money, food, water, energy or fuel;

(f) disruption of a system of communication;

(g) disruption of facilities for transport; or

(h) disruption of services relating to health.

(3) For the purposes of subsection (1)(b) an event or situation threatens damage to the environment only if it involves, causes or may cause–

(a) contamination of land, water or air with biological, chemical or radio-active matter, or

(b) disruption or destruction of plant life or animal life.

(4) The Chief Minister may by order amend subsection (2) so as to provide that in so far as an event or situation involves or causes disruption of a specified supply, system, facility or service–

(a) it is to be treated as threatening damage to human welfare, or

(b) it is no longer to be treated as threatening damage to human welfare.

(5) The event or situation mentioned in subsection (1) may occur or be inside or outside Gibraltar.

Power to make emergency regulations.

11.(1) The Minister may make emergency regulations if he is satisfied that the conditions in section 12 are satisfied.

(2) Regulations under this section must be prefaced by a statement by the person making the regulations–

(a) specifying the nature of the emergency in respect of which the regulations are made, and

(b) declaring that the person making the regulations–

(i) is satisfied that the conditions in section 12 are met;

(ii) is satisfied that the regulations contain only provision which is appropriate for the purpose of preventing, controlling or mitigating an aspect or effect of the emergency in respect of which the regulations are made;

(iii) is satisfied that the effect of the regulations is in due proportion to that aspect or effect of the emergency.

Conditions for making emergency regulations.

12.(1) This section specifies the conditions mentioned in section 11.

(2) The first condition is that an emergency has occurred, is occurring or is about to occur.

(3) The second condition is that it is necessary to make provision for the purpose of preventing, controlling or mitigating an aspect or effect of the emergency.

(4) The third condition is that the need for provision referred to in subsection (3) is urgent.

(5) For the purpose of subsection (3) provision which is the same as an enactment ("the existing legislation") is necessary if, in particular–

(a) the existing legislation cannot be relied upon without the risk of serious delay;

(b) it is not possible without the risk of serious delay to ascertain whether the existing legislation can be relied upon; or

(c) the existing legislation might be insufficiently effective.

(6) For the purpose of subsection (3) provision which could be made under an enactment other than section 11 ("the existing legislation") is necessary if, in particular–

(a) the provision cannot be made under the existing legislation without the risk of serious delay,

(b) it is not possible without the risk of serious delay to ascertain whether the provision can be made under the existing legislation, or

(c) the provision might be insufficiently effective if made under the existing legislation.

Scope of emergency regulations.

13.(1) Emergency regulations may make any provision which the person making the regulations is satisfied is appropriate for the purpose of preventing, controlling or mitigating an aspect or effect of the emergency in respect of which the regulations are made.

(2) In particular, emergency regulations may make any provision which the person making the regulations is satisfied is appropriate for the purpose of–

(a) protecting human life, health or safety,

(b) treating human illness or injury,

(c) protecting or restoring property,

(d) protecting or restoring a supply of money, food, water, energy or fuel,

(e) protecting or restoring a system of communication,

(f) protecting or restoring facilities for transport,

(g) protecting or restoring the provision of services relating to health,

(h) protecting or restoring the activities of banks or other financial institutions,

(i) preventing, containing or reducing the contamination of land, water or air,

(j) preventing, reducing or mitigating the effects of disruption or destruction of plant life or animal life,

(k) protecting or restoring the performance of public functions.

(3) Emergency regulations may make provision–

(a) to confer a function on a Minister or on any other specified person (and a function conferred may, in particular, be–

(i) a power, or duty, to exercise a discretion;

(ii) a power to give directions or orders (whether written or oral));

(b) provide for, subject to the Constitution, or enable the requisition or confiscation of property;

(c) provide for, subject to the Constitution, or enable the destruction of property, animal life or plant life;

(d) prohibit, or enable the prohibition of, movement to or from a specified place;

(e) require, or enable the requirement of, movement to or from a specified place;

(f) prohibit, or enable the prohibition of, assemblies of specified kinds, at specified places or at specified times;

(g) prohibit, or enable the prohibition of, travel at specified times;

(h) prohibit, or enable the prohibition of, other specified activities;

(i) create an offence of–

(i) failing to comply with a provision of the regulations;

(ii) failing to comply with a direction or order given or made under the regulations;

(iii) obstructing a person in the performance of a function under or by virtue of the regulations;

(j) disapply or modify an enactment or a provision made under or by virtue of an enactment;

(k) require a person or body to act in performance of a function (whether the function is conferred by the regulations or otherwise and whether or not the regulations also make provision for remuneration or compensation);

(l) confer jurisdiction on a court or tribunal (which may include a tribunal established by the regulations);

(m) make provision which applies generally or only in specified circumstances or for a specified purpose;

(n) make different provision for different circumstances or purposes.

(4) In subsection (3) "specified" means specified by, or to be specified in accordance with, the regulations.

Limitations of emergency regulations.

14.(1) Emergency regulations may make provision only if and in so far as the person making the regulations is satisfied–

(a) that the provision is appropriate for the purpose of preventing, controlling or mitigating an aspect or effect of the emergency in respect of which the regulations are made, and

(b) that the effect of the provision is in due proportion to that aspect or effect of the emergency.

(2) Emergency regulations may not–

(a) create an offence other than one of the kind described in section 13(3)(i),

(b) create an offence other than one which is triable only before a magistrates' court,

(c) create an offence which is punishable–

(i) with imprisonment for a period exceeding three months, or

(ii) with a fine exceeding level 5 on the standard scale, or

(d) alter procedure in relation to criminal proceedings.

(3) Emergency regulations may not amend this Part of this Act.

Duration.

15.(1) Emergency regulations shall lapse–

(a) at the end of the period of 30 days beginning with the date on which they are made, or

(b) at such earlier time as may be specified in the regulations.

(2) Subsection (1)–

(a) shall not prevent the making of new regulations, and

(b) shall not affect anything done by virtue of the regulations before they lapse.

Urgency.

16.(1) This section applies where–

(a) there is an urgent need to make provision of a kind that could be made by regulations under section 11(1); but

(b) there is insufficient time for the regulations to be made.

(2) The Chief Minister may by direction make provision of a kind that could be made by regulations under section 11(1).

(3) A direction under subsection (2) shall be in writing.

(4) Where the Chief Minister gives a direction under subsection (2)–

(a) he may revoke or vary the direction by further direction,

(b) he shall revoke the direction as soon as is reasonably practicable (and he may, if or in so far as he thinks it desirable, re-enact the substance of the direction by way of regulations under section 11(1)), and

(c) the direction shall cease to have effect at the end of the period of 7 days beginning with the day on which it is given (but without prejudice to the power to give a new direction).

(5) A provision of a direction under subsection (2) shall be treated for all purposes as if it were a provision of regulations made under section 11(1).

(6) Sections 12, 13 and 14 shall apply when a direction is made under subsection (2).

PART 4
Civil Contingencies Committee

Establishment of Civil Contingencies Committee.

17.(1) There shall be established a Civil Contingencies Committee ("the Committee").

(2) The Committee shall comprise such members as the Chief Minister may, by notice in the Gazette, specify.

(3) The Chairman of the Committee shall be the Chief Minister, and in his absence the Minister with responsibility for Civil Contingencies and in his absence any person that the latter may designate.

(4) The Committee shall have the staff and resources that the Government may from time to time provide.

Role and functions of the Committee.

18.(1) The role and function of the Committee shall be as follows:–

(a) to advise the Government on any matter relating to civil contingencies and emergencies of all kinds, to draw up plans to pre-empt such contingencies and to deal with their consequences if they should occur;

(b) to co-ordinate the roles and activities of government departments, agencies, authorities, companies, and other authorities and persons in response to a civil contingency;

(c) to organise and conduct exercises for the rehearsal and testing of civil contingency plans;

(d) such other roles and functions as the Minister may designate in writing.

(2) In discharging its duties under subsection (1) the Civil Contingencies Committee must take into consideration all necessary measures to ensure the protection and safety of persons with disabilities in situations of risk.

Appointment of Civil Contingencies Coordinator.

19.(1) The Government may designate a suitably qualified or experienced person to be the Civil Contingencies Coordinator and to organise and direct the work and functions of the Committee.

(2) The Government may appoint such other persons as it thinks necessary or desirable to assist and support the Civil Contingencies Coordinator.

Regulations.

20.(1) The Minister may make such regulations as he thinks fit in relation to the carrying out by the Committee, the Coordinator or other staff of its or their roles and functions, the duties and obligations of others in relation to the Committee and such other matters as he considers necessary to enable the Committee to function effectively.

PART 5
European Critical Infrastructures

Interpretation.

21. In this Part−

"critical infrastructure" means an asset, system or part thereof located in Gibraltar 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 Gibraltar as a result of the failure to maintain those functions;

"the Directive" means 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, as the same may be amended from time to time;

"European critical infrastructure" or "ECI" means critical infrastructure located in Gibraltar the disruption or destruction of which would have a significant impact in at least Gibraltar and a Member State and the significance of the impact shall be assessed in terms of cross-cutting criteria which must include effects resulting from cross-sector dependencies on other types of infrastructure;

"owners or operators of ECIs" means those entities responsible for investments in, or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Part;

"protection" means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;

"risk analysis" means consideration of relevant threat scenarios in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;

"sensitive critical infrastructure protection related information" means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations.

Identification of ECIs.

22.(1) The Government must, in accordance with the procedure referred to in section 23, identify potential European Critical Infrastructures in Gibraltar which−

(a) satisfy the cross-cutting and sectoral criteria set out in this section; and

(b) meet the criteria in the definitions of the terms "critical infrastructure" and "European critical infrastructure" in section 21.

(2) The cross-cutting criteria referred to in subsection (1) shall comprise the following−

(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(b) economic effects criterion (assessed in terms of the significance of economic loss or degradation of products or services, including potential environmental effects);

(c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services).

(3) The cross-cutting criteria thresholds must be based on the severity of the impact of the disruption or destruction of a particular infrastructure and the precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Government.

(4) The Government shall ensure that the European Commission is informed on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

(5) The sectoral criteria must–

(a) take into account the characteristics of individual ECI sectors; and

(b) be classified.

(6) The Government may use such guidelines for−

(a) the application of the cross-cutting and sectoral criteria; and

(b) approximate thresholds to be used for the purposes of identifying ECIs,

as are developed pursuant to Article 3 of the Directive.

(7) The following sectors and subsectors shall be subject to this Part−

(a) the energy sector which is divided into the following subsectors−

(i) electricity, comprising infrastructures and facilities for generation and transmission of electricity in respect of supply of electricity,

(ii) oil, comprising oil production, refining, treatment, storage and transmission by pipelines,

(iii) gas, comprising gas production, refining, treatment, storage and transmission by pipelines, and LNG terminals; and

(b) the transport sector which is divided into the following subsectors−

(i) road transport,

(ii) air transport,

(iii) ocean and short-sea shipping, and

(iv) ports.

Procedure for the identification of critical infrastructures which may be designated as an ECI.

23.(1) When identifying the critical infrastructures which may be designated as an ECI (the "potential ECI"), the Government must follow the procedure set out in Schedule 2.

(2) A potential ECI which has passed through the procedure set out in Schedule 2 shall only be communicated to Member States which may be significantly affected by the potential ECI.

Designation of ECIs.

24.(1) The Government must inform a Member State which may be significantly affected by a potential ECI about its identity and the reasons for its designation as a potential ECI.

(2) Where a potential ECI is located in Gibraltar, the Government must–

(a) engage in discussions with any Member State which may be significantly affected by the potential ECI; and

(b) designate it as an ECI following an agreement between the Government and the Member States which may be significantly affected.

(3) Where a designated ECI is located in Gibraltar, the Government shall ensure that the European Commission is informed on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated ECI and only the Member State which may be significantly affected by an ECI shall know its identity.

(4) Where an ECI is located in Gibraltar, the Government shall inform the owner or operator of the infrastructure that the infrastructure has been designated as an ECI and such information shall be classified at an appropriate level.

(5) The process of identifying and designating ECIs under this Part must be–

(a) completed as soon as possible after the coming into operation of this Part; and

(b) reviewed on a regular basis.

Operator security plans.

25.(1) The operator security plan ('OSP') procedure shall–

(a) identify the critical infrastructure assets of the ECI;

(b) identify the security solutions that exist or are being implemented for their protection; and

(c) cover, as a minimum, the information set out in section 26.

(2) The Government must assess whether each designated ECI located in Gibraltar possesses an OSP or has in place equivalent measures addressing the issues identified in section 26.

(3) If the Government finds that an OSP or equivalent measures exist and are updated regularly, no further implementation action shall be necessary.

(4) If the Government finds that an OSP or equivalent measures have not been prepared, it shall ensure, by any measures it deems appropriate, that the OSP or equivalent measures are prepared addressing the issues identified in section 26.

(5) The Government must ensure that the OSP or equivalent measures are in place and are reviewed regularly within one year following designation of the critical infrastructure as an ECI.

(6) The period referred to in subsection (5) may be extended in exceptional circumstances.

(7) The Government shall ensure that the European Commission is notified of any extension granted pursuant to subsection (6).

(8) Compliance with any measure, including a European Union measure, which in a particular sector−

(a) requires, or refers to a need to have, a plan similar or equivalent to an OSP; and

(b) oversight by the relevant authority of such a plan,

shall be deemed to satisfy all the requirements under this section.

ECI OSP Procedure.

26.(1) The ECI OSP procedure must cover at least the following matters−

(a) the identification of important assets;

(b) the conduct of a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and

(c) the identification, selection and prioritisation of counter-measures and procedures with a distinction between−

(i) permanent security measures which identify indispensable security investments and means which are relevant to be employed at all times and this heading must include the further information set out in subsection (2); and

(ii) graduated security measures, which can be activated according to varying risk and threat levels.

(2) The further information referred to in subsection (1)(c)(i) is information concerning−

(a) general measures such as technical measures (including installation of detection, access control, protection and prevention means);

(b) organisational measures (including procedures for alerts and crisis management);

(c) control and verification measures;

(d) communication;

(e) awareness raising and training; and

(f) security of information systems.

Security Liaison Officers.

27.(1) Every designated ECI in Gibraltar must have a Security Liaison Officer or equivalent who shall act as the point of contact for security related issues between the owner or operator of the ECI and the Government.

(2) The Government must assess whether each designated ECI located in Gibraltar possesses a Security Liaison Officer or equivalent.

(3) If the Government finds that a Security Liaison Officer is in place or an equivalent exists, no further implementation action shall be necessary.

(4) If the Government finds that a Security Liaison Officer or equivalent does not exist in relation to a designated ECI, it shall ensure, by any measures it deems appropriate, that such a Security Liaison Officer or equivalent is designated.

(5) The Government must implement an appropriate communication mechanism between the Government and the Security Liaison Officer or equivalent with the objective of

exchanging relevant information concerning identified risks and threats in relation to the ECI concerned and this communication mechanism shall be without prejudice to the requirements concerning access to sensitive and classified information.

(6) Compliance with any measure, including a European Union measure, which in a particular sector requires, or refers to a need to have, a Security Liaison Officer or equivalent, shall be deemed to satisfy all the requirements under this section.

Reporting.

28.(1) The Government must conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure in Gibraltar as an ECI within those subsectors.

(2) The Government shall ensure that every two years a classified report is sent to the European Commission containing generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated under section 24.

Sensitive European critical infrastructure protection-related information.

29.(1) Any person handling classified information under this Part on behalf of the Government must have an appropriate level of security vetting.

(2) The Government must ensure that sensitive European critical infrastructure protection-related information submitted to it is not used for any purpose other than the protection of critical infrastructures.

(3) This section shall also apply to non-written information exchanged during meetings at which sensitive subjects are discussed.

European critical infrastructure protection contact points.

30.(1) The Government shall appoint a European critical infrastructure protection contact point ('ECIP contact point').

(2) The ECIP contact point shall coordinate European critical infrastructure protection issues within Gibraltar and shall have such other functions as the Government may prescribe.

(3) The appointment of an ECIP contact point does not preclude other relevant authorities in Gibraltar from being involved in European critical infrastructure protection issues.

PART 6

Regulations.

31.(1) The Government may make regulations for the implementation of any European Union measure.

(2) Section 23(b) of the Interpretation and General Clauses Act shall not apply to any penalty imposed in any regulations made under subsection (1).

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) *Deleted*

(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 section 31 of the Communications Act 2006;

(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) Part 5;

(b) the Communications (Combatting Child Pornography) Regulations 2013 or the Child Victims of Sexual Abuse and Exploitation Regulations 2013; and

(c) the Crimes Act 2011.

(4) The Competent Authority may share information with the Gibraltar CSIRT, and any relevant European Union or United Kingdom authority 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 retained sector-specific European Union law; or

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

then the provisions of that retained 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 the Gibraltar GDPR.

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;

"Information Commissioner" means the Commissioner designated under section 123 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 as it had effect immediately before 1 January 2021 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 Cooperation Group" means the Cooperation Group established under Article 11(1) of the NIS Directive;

"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 section 2 of the Communications Act 2006;

(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 as it had effect immediately before 1 January 2021;

"online marketplace" means a digital service that allows consumers and/or traders as respectively defined in the Consumer (Alternative Dispute Resolution) Regulations 2015 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 Gibraltar explicitly designated to act on behalf of a digital service provider not established in Gibraltar, 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) *Deleted*

(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).

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).

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.

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 fulfil the requirements of this Part, the Competent Authority may if it considers it appropriate liaise with –

(a) the relevant authorities in any Member States or the United Kingdom;

(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) *Deleted*

(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 Information Commissioner and any other relevant data protection authorities when addressing incidents resulting in personal data breaches.

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) *Deleted*

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

(d) *Deleted*

(4) The Gibraltar CSIRT may co-operate with or participate in international co-operation networks (including the CSIRTs network) if the Gibraltar CSIRT considers it appropriate to do so.

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.

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 in a notification under subsection (1), the Competent Authority may inform the relevant authorities in any affected Member States or the United Kingdom if the Competent Authority considers that the incident has a significant impact on the continuity of essential services in that Member State or the United Kingdom.

(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 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 Gibraltar.

(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.

(6A) The digital service provider must have regard to any relevant guidance published by the Competent Authority.

(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) *Deleted*

(10) The Competent Authority is not required to share information under this Act 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) *Deleted*

(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) The Competent Authority may give information and assistance to, and otherwise co-operate with, a competent authority in a Member State or in the United Kingdom if the Competent Authority considers that to do so would be in the interest of effective supervision of digital service providers (whether inside or outside Gibraltar) including in the event of an incident notified under section 43(3).

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) *Omitted*

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 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.

(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.

SCHEDULE 1

Sections 4, 6, 7, 9

Any airline operating an air service to Gibraltar

Any dispensing chemist or pharmacy

Any-

government department,
wholly owned government company
company that is wholly owned by the government jointly with a statutory authority or body
statutory authority or agency,
public officer or any employee or officer of any of the abovementioned entities

Any operator of a route bus service

Any owner or operator of tour buses

Any person/entity who provides a public electronic communications network which makes telephone services available (whether for spoken communication or for the transmission of data)

Any school in Gibraltar

Any shipping company operating a passenger or cargo service to Gibraltar

Any taxi licensee

AquaGib Limited

City Fire Brigade

Customs Department

Gibraltar Broadcasting Corporation

Gibraltar Community Projects Limited

Land Property Services Limited

Royal Gibraltar Post Office

Security and Immigration Limited

St John's Ambulance

Terminal Management Limited

The Chief Environmental Health Officer

The Director of Public Health

The Environmental Agency Limited

The Gibraltar Bus Company Limited

The Gibraltar Electricity Authority

The Gibraltar Health Authority

The Gibraltar Port Authority

The Port Medical Officer

The Principal Immigration Officer

The Royal Gibraltar Police (save in relation to matters appertaining to internal security or law enforcement)

SCHEDULE 2

Section 23

In identifying critical infrastructures which may be designated as an ECI, the Government must apply the following sequential steps−

(1) in Step 1, the sectoral criteria in order to make a first selection of critical infrastructures within a sector.

(2) in Step 2, the definition of the term critical infrastructure in section 21 to the potential ECI identified under Step 1. The significance of the impact must be determined either by using Gibraltar's own methods for identifying critical infrastructures or with reference to the cross-cutting criteria, at an appropriate Gibraltar level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption or recovery must be taken into account;

(3) in Step 3, the transboundary element of the definition of ECI in section 21 to the potential ECI that has passed the first two steps of this procedure. A potential ECI which does satisfy the definition must follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption or recovery must be taken into account.

(4) in Step 4, the cross-cutting criteria to the remaining potential ECIs and the cross-cutting criteria must take into account−

(a) the severity of impact;

(b) for infrastructure providing an essential service, the availability of alternatives; and

(c) the duration of disruption or recovery or both,

A potential ECI which does not satisfy the cross-cutting criteria must not be considered to be an ECI.

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 and the CSIRTs network.

(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) *Deleted*

(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.

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).

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