



STATUTORY INSTRUMENTS.

**S.I. No. 360 of 2018**



EUROPEAN UNION (MEASURES FOR A HIGH COMMON LEVEL OF  
SECURITY OF NETWORK AND INFORMATION SYSTEMS)  
REGULATIONS 2018

EUROPEAN UNION (MEASURES FOR A HIGH COMMON LEVEL OF  
SECURITY OF NETWORK AND INFORMATION SYSTEMS)  
REGULATIONS 2018

CONTENTS

Regulations

*PART 1*

GENERAL PROVISIONS

1. Citation
2. Interpretation
3. Application
4. Safeguarding of State's essential functions
5. Sharing of Information
6. Co-operation with Data Protection Commission and the Garda Síochána

*PART 2*

COMPETENT AUTHORITY, SINGLE POINT OF CONTACT, CSIRT

7. Competent authority for operators of essential services
8. Competent authority for digital service providers
9. Single Point of Contact
10. CSIRT

*PART 3*

NATIONAL STRATEGY ON SECURITY OF NETWORK AND  
INFORMATION SYSTEMS

11. National Strategy on the security of network and information systems

*PART 4*

OPERATORS OF ESSENTIAL SERVICES

12. Designation of Operators of Essential Services
13. Procedure for designation as operator of essential services

14. Amendment of designation as operator of essential services by addition of sector, subsector or essential service in respect of which a person is designated
15. Amendment of designation as operator of essential services by cancellation of category of sector or subsector or essential service in respect of which a person is designated
16. Register of Operators of Essential Services, Combined Operators Register
17. Security requirements in respect of operators of essential services
18. Incident notification by operators of essential services

*PART 5*

DIGITAL SERVICE PROVIDERS

19. Definition
20. Relevant digital service provider
21. Security measures to be taken by relevant digital service providers
22. Incident notification by a relevant digital service provider
23. Co-operation and assistance in respect of relevant digital service providers whose network and information systems are not in State
24. Co-operation in respect of digital service providers whose main establishment or designated representative not in State but whose network and information systems are in State

*PART 6*

GUIDELINES

25. Guidelines

*PART 7*

VOLUNTARY NOTIFICATION

26. Voluntary Notification

*PART 8*

IMPLEMENTATION AND ENFORCEMENT

27. Security assessment
28. Appointment of authorised officers
29. Powers of authorised officers

4 [360]

30. Compliance notice
31. Information notice
32. Service of documents
33. Offence by body corporate
34. Penalties
35. Costs of prosecutions
36. Prosecution of offences-operators of essential services
37. Prosecution of offences-digital service providers
38. Hearing of proceedings otherwise than in public

SCHEDULE 1

SCHEDULE 2

S.I. No. 360 of 2018

EUROPEAN UNION (MEASURES FOR A HIGH COMMON LEVEL OF  
SECURITY OF NETWORK AND INFORMATION SYSTEMS)  
REGULATIONS 2018

I, DENIS NAUGHTEN, Minister for Communications, Climate Action and Environment, in exercise of the powers conferred on me by section 3 of the European Communities Act 1972 (No. 27 of 1972) and for the purpose of giving effect to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016<sup>1</sup>, hereby make the following regulations:

PART 1

GENERAL PROVISIONS

*Citation*

1. These Regulations may be cited as the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018.

*Interpretation*

2. (1) In these Regulations—

“authorised officer” means a person appointed under Regulation 28;

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

“Combined Operators Register” means the register referred to in Regulation 16(5);

“Commission” means the European Commission;

“competent authority” in relation to—

- (a) an operator of essential services, means the person designated as a competent authority in the State under Regulation 7(1) or (2) in respect of the sectors referred to in Regulation 7(1) or (2), as the case may be, and
- (b) a digital service provider, means the person designated as a competent authority in the State under Regulation 8;

<sup>1</sup>O.J. No. L 194, 19.7.2016, p. 1

*Notice of the making of this Statutory Instrument was published in  
“Iris Oifigiúil” of 21st September, 2018.*

“competent authority in another member state” means any person designated as a competent authority by a member state (other than the State) for the purposes of the Directive;

“Co-operation Group” means the Co-operation Group referred to in Article 11 of the Directive;

“CSIRT” has the meaning assigned to it by Regulation 10;

“CSIRT in another member state” means any authority or body designated as a computer security incident response team by a member state (other than the State) for the purposes of the Directive;

“CSIRTs network” means the network of national computer security incident response teams referred to in Article 12 of the Directive;

“Data Protection Regulation” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016<sup>2</sup> on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation);

“digital service” has the meaning assigned to it by Regulation 19;

“digital service provider” means a legal person who provides a digital service;

“Directive” means Directive 2016/1148 of the European Parliament and of the Council of 06 July 2016<sup>3</sup> concerning measures for a high common level of security of network and information systems across the Union;

“Domain Name System” means a hierarchical distributed naming system in a network which refers queries for domain names;

“DNS service provider” means an entity which provides domain name services on the internet;

“enactment” means—

- (a) an Act of the Oireachtas,
- (b) a statute that was in force in Saorstát Éireann immediately before the date of the coming into operation of the Constitution and that continues in force by virtue of Article 50 of the Constitution, or
- (c) an instrument made under an Act of the Oireachtas or a statute referred to in paragraph (b);

“ENISA” means the European Union Agency for Network and Information Security;

<sup>2</sup>O.J. No. L 119, 4.5.2016, p.1

<sup>3</sup>O.J. No. L 194, 19.7.2016, p.1

“essential service” means a service provided in the State which is essential for the maintenance of critical societal activities or critical economic activities, or both, in the State and which is included in the essential services list prepared and maintained by a competent authority under Regulation 12(3);

“European act” has the meaning given to it by section 8(3) of the European Union Act 2009 (No. 33 of 2009);

“Implementing Regulation” means Commission Implementing Regulation (EU) 2018/151 of 30 January 2018<sup>4</sup> laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact;

“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” or “IXP” means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an internet exchange point provides interconnection only for autonomous systems; an internet exchange point 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;

“Minister” means the Minister for Communications, Climate Action and Environment;

“national strategy on the security of network and informations systems” means the national strategy prepared by the Minister under Regulation 11;

“network and information system” means:

- (a) an electronic communications network within the meaning of Regulation 2 of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011(S.I. No. 333 of 2011),
- (b) any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data, or
- (c) digital data stored, processed, retrieved or transmitted by elements referred to in paragraph (a) or (b) for the purposes of the operation, use, protection and maintenance of the data;

<sup>4</sup>O.J. No. L 26, 31.1.2018, p.48

“online marketplace” means a digital service that allows consumers or traders, or both, as respectively defined in the European Union (Alternative Dispute Resolution for Consumer Disputes) Regulations 2015 (S.I. No. 343 of 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 a person designated as an operator of essential services under Regulation 12;

“Operators Register” means the Register of Operators of Essential Services established and maintained by a competent authority under Regulation 16;

“personal data” means personal data within the meaning of—

- (a) the Data Protection Regulation, or
- (b) Part 5 of the Data Protection Act 2018 (No. 7 of 2018);

“personal data breach” means a personal data breach under—

- (a) the Data Protection Regulation, or
- (b) Part 5 of the Data Protection Act 2018;

“relevant authority in another member state” has the meaning assigned to it by Regulation 9;

“relevant digital service provider” has the meaning assigned to it by Regulation 20;

“representative” means any natural or legal person established in the State which is explicitly designated by a digital service provider which is not established in the Union to act on behalf of the digital service provider in respect of the provision by that digital service provider of its digital services in the Union;

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

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



“single point of contact” means the person designated as the single point of contact in the State under Regulation 9;

“single point of contact in another member state” means the person designated as the single point of contact in a member state (other than the State) for the purposes of the Directive;

“top-level domain name registry” means an entity which administers and operates the registration of internet domain names under a specific top-level domain;

“Union” means the European Union.

(2) A word or expression which is used in these Regulations and which is also used in the Directive has, unless the context otherwise requires, the same meaning in these Regulations as it has in the Directive.

#### *Application*

3. (1) These Regulations, other than Regulation 26, apply in respect of operators of essential services and digital service providers.

(2) Regulation 17 shall not apply in respect of an operator of essential services in any of the following sectors:

- (i) the sector referred to in number 3 of column (1) of Schedule 1
- (ii) the sector referred to in number 4 of column (1) of Schedule 1.

(3) These Regulations are without prejudice to the European Union (Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography) Regulations 2015 (S.I. No. 309 of 2015) and the Criminal Justice (Offences relating to Information Systems) Act 2017 (No. 11 of 2017).

#### *Safeguarding of State’s essential functions*

4. Nothing in these Regulations shall prejudice the ability of the State to safeguard its essential functions, in particular its national security, including taking action to protect information the disclosure of which is considered by the competent authority referred to in Regulation 7(1) to be contrary to the State’s essential security interests, the maintenance of law and order and, in particular, to allow for the investigation, detection and prosecution of criminal offences.

#### *Sharing of information*

5. (1) Information may be shared by a competent authority, the CSIRT or the single point of contact in accordance with these Regulations.

(2) Information shared in accordance with these Regulations may include personal data.

(3) Where a competent authority, the CSIRT or the single point of contact shares information under these Regulations in relation to an operator of essential services or a digital service provider, the competent authority, CSIRT or

single point of contact, as the case may be, shall take all reasonable steps to protect the confidentiality of the information so shared and the network and information security and commercial interests of the operator of essential services or the digital service provider to which the information relates.

*Co-operation with Data Protection Commission and the Garda Síochána*

6. (1) The single point of contact and a competent authority shall consult and co-operate with, including, where necessary, by sharing information with, the Data Protection Commission where the Data Protection Regulation or the Data Protection Acts 1988 to 2018 apply in relation to any matter concerning these Regulations, including in relation to an incident resulting in a personal data breach in which case the competent authority shall work in close co-operation with the Data Protection Commission in addressing the incident.

(2) The single point of contact and a competent authority shall, in accordance with law, consult and co-operate with, including, where necessary, by sharing information with, the Garda Síochána in relation to any matter to which these Regulations apply.

## PART 2

### COMPETENT AUTHORITY, SINGLE POINT OF CONTACT, CSIRT

*Competent authority for operators of essential services*

7. (1) The Minister is for the purposes of these Regulations designated as the competent authority in the State on the security of network and information systems in respect of operators of essential services in the sectors set out in Schedule 1 other than—

- (a) the sector set out at number 3 of column (1) of Schedule 1, and
- (b) the sector set out at number 4 of column (1) of Schedule 1.

(2) The Central Bank of Ireland is for the purposes of these Regulations designated as the competent authority in the State on the security of network and information systems in respect of operators of essential services in the following sectors:

- (i) the sector set out at number 3 of column (1) of Schedule 1
- (ii) the sector set out at number 4 of column (1) of Schedule 1.

(3) A competent authority referred to in paragraph (1) or (2) shall, in respect of each sector in respect of which it is designated as the competent authority—

- (a) review the application of these Regulations to the extent to which they apply in respect of the sector,

and

- (b) co-operate with the single point of contact and the CSIRT in accordance with these Regulations.

*Competent authority for digital service providers*

8. (1) The Minister is for the purposes of these Regulations designated as the competent authority in the State in respect of digital service providers.

(2) The competent authority designated under paragraph (1) shall in respect of digital service providers—

- (a) review the application of these Regulations,

and

- (b) co-operate with the single point of contact and the CSIRT in accordance with these Regulations.

*Single Point of Contact*

9. (1) The Minister is designated as the single point of contact in the State for the purposes of these Regulations.

(2) The single point of contact shall—

- (a) liaise with a relevant authority in another member state, the Co-operation Group and the CSIRTs network to ensure cross-border co-operation in relation to the Directive and these Regulations,

and

- (b) co-operate with a competent authority and the CSIRT in accordance with these Regulations.

(3) The single point of contact shall in each year after the year in which these Regulations come into operation submit reports to the Co-operation Group in relation to incident notifications made to the CSIRT under Regulations 18 and 22, including the number of notifications, the nature of the notified incidents and the actions taken under the relevant Regulation.

(4) In this Regulation, “relevant authority in another member state” means one or more of the following:

- (a) a competent authority in another member state;
- (b) the single point of contact in another member state;
- (c) the CSIRT in another member state.

*CSIRT*

10. (1) The unit of the Department of Communications, Climate Action and Environment known as the computer security incident response team (in these Regulations referred to as the “CSIRT”) is for the purpose of these Regulations

designated as the computer security incident response team in the State in respect of the sectors set out in Schedule 1 and the services set out in Schedule 2.

(2) The CSIRT is responsible for risk and incident handling in accordance with a well-defined process in respect of the sectors set out in Schedule 1 and the services set out in Schedule 2 and, for that purpose, shall—

- (a) monitor incidents within the State,
- (b) provide early warnings, alerts, announcements and dissemination of information about risk and incidents to relevant stakeholders,
- (c) respond to incidents notified to it under Regulation 18 or 22,
- (d) provide dynamic risk and incident analysis and situational awareness,
- (e) participate and co-operate in the CSIRTs network,
- (f) establish relationships with persons in the private sector to facilitate co-operation with that sector,
- (g) for the purpose of facilitating co-operation, promote the adoption and use of common or standardised practices for—
  - (i) incident and risk handling procedures, and
  - (ii) incident, risk and information classification schemes,

and

- (h) co-operate with a competent authority and the single point of contact in accordance with these Regulations.

(3) For the purpose of performing its functions under these Regulations, the CSIRT shall ensure that—

- (a) there is a high level of availability of its communications services by avoiding single points of failure and that there are several means by which it can be contacted by, and can make contact with, others,
- (b) communications channels are clearly specified and well known to constituency and cooperative partners,
- (c) its premises and supporting information systems are located in secure sites,

and

- (d) in relation to business continuity—
  - (i) it is equipped with an appropriate system for managing and routing requests in order to facilitate handovers,

- (ii) it is adequately staffed to ensure availability at all times, and
  - (iii) it relies on an infrastructure the continuity of which is ensured with redundant systems and backup working space being available.
- (4) Where it considers it appropriate to do so, the CSIRT may co-operate with international co-operation networks.
- (5) In this Regulation, “relevant stakeholders” includes—
- (a) a Minister of the Government, and
  - (b) a body, or holder of an office, in whom functions are vested relating to the regulation of persons or activities referred to in Schedule 1 or the services referred to in Schedule 2 for purposes other than the purposes of these Regulations where the body or office is established by or under an enactment,

where the CSIRT considers that, having regard to its functions and the functions of the Minister concerned or the functions of the body or office holder concerned, as the case may be, the provision of the warnings, alerts announcements or information concerned, is appropriate in the circumstances.

### PART 3

#### NATIONAL STRATEGY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

##### *National Strategy on the security of network and information systems*

11. (1) The Minister shall prepare a national strategy on the security of network and information systems (the “national strategy”).

(2) The national strategy shall set out strategic objectives and policy and regulatory measures intended to achieve and maintain a high level of security of network and information systems in not fewer than the sectors referred to in Schedule 1 and the services referred to in Schedule 2 and shall address the following:

- (a) the objectives and priorities of the national strategy;
- (b) the regulatory measures and enforcement framework required to achieve the objectives and priorities of the national strategy including setting out the roles and responsibilities of governmental bodies and other relevant persons;
- (c) measures relating to preparedness, response and recovery in relation to risks and incidents, including co-operation between the public and private sectors;

- (d) education, awareness-raising and training programmes relating to the national strategy;
  - (e) research and development plans relating to the national strategy;
  - (f) the development of a risk assessment plan to identify any risks relating to network and information systems;
  - (g) a list of the various persons involved in the implementation of the national strategy.
- (3) The Minister may publish on the internet in such form and in such manner as he or she considers appropriate a draft of the proposed national strategy.
- (4) Where a draft of the proposed national strategy is published in accordance with paragraph (3), a person may make written submissions or representations to the Minister in relation to the draft within a period of 30 working days from the date on which that draft is published.
- (5) The Minister shall consider any submissions or representations made to him or her under paragraph (4).
- (6) The first national strategy shall be adopted within nine months of the day on which these Regulations come into operation.
- (7) The Minister shall cause a copy of the national strategy to be laid before each House of the Oireachtas and, not more than 5 working days after the national strategy is so laid before the Houses of the Oireachtas, the Minister shall cause it to be published on the internet in such form and in such manner as the Minister considers appropriate.
- (8) The Minister may review the national strategy at any time and, in any event, shall review it not later than 4 years after the date of its first adoption and thereafter on every fourth anniversary of that date.
- (9) Where, after carrying out a review referred to in paragraph (8), the Minister decides to revise the national strategy, paragraphs (3) to (5) and (7) shall apply, with necessary modification, in respect of any such revision.
- (10) The Minister may, in preparing the national strategy or any revisions thereto, request the assistance of ENISA.

#### PART 4

#### OPERATORS OF ESSENTIAL SERVICES

##### *Designation of Operators of Essential Services*

12. (1) A competent authority shall designate a person as an operator of essential services in respect of an essential service in a sector in respect of which the competent authority is designated as the competent authority where that competent authority is satisfied that—

- (a) the person provides the essential service in the State,
  - (b) the person has an establishment in the State,
  - (c) the person is a person of a type set out in Column (3) of Schedule 1,
  - (d) the sector and, where appropriate, subsector in which the essential service is provided are each a sector and subsector set out in Schedule 1;
  - (e) the provision by the person of the essential service depends on network and information systems, and
  - (f) an incident affecting the provision by the person of the essential service would have significant disruptive effects on the provision of that service in the State.
- (2) Where an operator of essential services is—
- (a) an undertaking which is subject to the requirements of Regulations 23 and 24 of the European Communities (Electronic Communications Network and Services) (Framework) Regulations 2011 (S.I. No. 333 of 2011), or
  - (b) a trust service provider subject to the requirements of Article 19 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014<sup>5</sup> on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,

these Regulations shall apply to the operator in respect only of the service in respect of which it is designated as an operator of essential services.

(3) For the purpose of designating a person as an operator of essential services under paragraph (1), a competent authority shall prepare and maintain a list of services in the sectors in respect of which it is designated as the competent authority which that competent authority is satisfied are essential for the maintenance of critical societal activities or critical economic activities, or both, in the State (the “essential services list”).

(4) The essential services list shall be reviewed and updated by the competent authority concerned from time to time and, in any event, not later than 9 November 2020 and, thereafter, not later than every second anniversary of that date.

(5) In determining the significance of a disruptive effect referred to in paragraph (1) (f) insofar as it relates to the provision by a person of an essential service in the State, a competent authority shall, where it considers it appropriate to do so, take into account factors specific to the sector to which the

<sup>5</sup>O.J. No. L 257, 28.8.2014, p.73

person providing the service belongs and, in every case, shall take into account the following:

- (a) the number of users relying on the service provided by the person;
- (b) the extent to which other sectors set out in Schedule 1 depend on the service provided by the person;
- (c) the impact that an incident could have in terms of degree and duration on economic or societal activities or public safety;
- (d) the market share of the service provided by the person;
- (e) the geographic spread with regard to the area that may be affected by an incident;
- (f) the importance of the person in the maintenance of a sufficient level of the service in the State taking into account the availability of alternative means for the provision of the service concerned.

(6) A person may be designated under paragraph (1) in respect of one or more category of sector, subsector or essential service.

*Procedure for designation as operator of essential services*

13. (1) In considering whether a person may be required to be designated as an operator of essential services, a competent authority may request information from the person which the competent authority reasonably believes it requires for the purpose of deciding whether to designate that person as an operator of essential services.

(2) Where a competent authority proposes to designate a person as an operator of essential services, the competent authority shall notify the person in writing accordingly—

- (a) stating the reasons why the person is proposed to be designated,
- (b) specifying the category of sector and, where appropriate, subsector and the essential service in respect of which the person is to be so designated, and
- (c) giving the person an opportunity to make representations in writing to the competent authority in respect of the proposed designation within 15 working days of the date of the notification.

(3) The competent authority shall consider any representations made by a person under paragraph (2) and shall, within 20 working days of the earlier of—

- (a) the receipt of the representations, or
- (b) the expiration of the period referred to in paragraph (2)(c),



decide whether to designate the person as an operator of essential services in respect of a particular category of sector, subsector or essential service.

(4) Where a competent authority decides to designate a person as an operator of essential services, the competent authority shall notify the person in writing stating—

- (a) that that person is so designated,
- (b) the category of sector and, where appropriate, subsector and the essential service in respect of which that person is so designated, and
- (c) where that person has made representations in accordance with paragraph (2), the reasons why that person is so designated.

(5) Where a person, in addition to providing an essential service in the State, provides the essential service in another member state, the competent authority shall consult with the competent authority in that member state before deciding whether to designate the person as an operator of essential services in respect of that service.

(6) A competent authority shall promptly enter particulars of a person designated by it as an operator of essential services in the Operators Register maintained by the competent authority under Regulation 16.

*Amendment of designation as operator of essential services by addition of sector, subsector or essential service in respect of which a person is designated*

14. (1) A competent authority shall add a new category of sector or subsector set out in the Schedule, or an essential service, to the category of sector or, where appropriate, subsector or the essential service in respect of which a person is designated as an operator of essential services where the competent authority is satisfied that Regulation 12 is complied with in respect of that additional category of sector or subsector or essential service.

(2) Before a competent authority makes an addition referred to in paragraph (1), the competent authority may request information from the operator of essential services concerned which the competent authority reasonably believes it requires for the purpose of deciding whether to make the addition.

(3) Where a competent authority proposes to make an addition referred to in paragraph (1), it shall notify the operator of essential services concerned in writing accordingly—

- (a) stating the reasons for the proposed addition,
- (b) stating the nature of the proposed addition, and
- (c) giving the operator an opportunity to make representations in writing to the competent authority in respect of the proposed addition within 15 working days of the date of the notification.

(4) The competent authority shall consider any representations made by the operator of essential services in accordance with paragraph (3) and shall, within 20 working days of the earlier of—

(a) the receipt of the representations, or

(b) the expiration of the period referred to in that paragraph,

decide whether to make the addition.

(5) Where the competent authority decides to make the addition, it shall notify the operator of essential services concerned in writing accordingly.

(6) Where an addition referred to in paragraph (1) is made, the competent authority making the addition shall promptly amend the Operators Register maintained by it under Regulation 16 accordingly and where the addition is made by the competent authority referred to in Regulation 7(2) a copy of the amended Operators Register maintained by that competent authority shall be promptly furnished to the competent authority referred to in Regulation 7(1) who shall amend the Combined Operators Register accordingly.

*Amendment of designation as operator of essential services by cancellation of category of sector or subsector or essential service in respect of which a person is designated*

15. (1) A competent authority shall cancel a category of sector or, where appropriate, subsector or an essential service from the category of sector or subsector or essential service in respect of which a person is designated as an operator of essential services where the competent authority is satisfied that the person no longer complies with Regulation 12 in respect of that category of sector or subsector or the essential service.

(2) An operator of essential services who is of the view that it is no longer appropriate for it to be designated as an operator of essential services in respect of a particular category of sector or subsector or essential service may notify the competent authority in writing accordingly setting out the reasons why the operator is of that view and requesting cancellation accordingly.

(3) Before a competent authority makes a cancellation, the competent authority may request information from the operator of essential services concerned which that competent authority reasonably requires for the purpose of deciding whether to make the cancellation.

(4) Where a competent authority proposes—

(a) to make a cancellation, or

(b) to refuse a request for cancellation made under paragraph (2),

it shall notify the operator of essential services concerned in writing accordingly—

- (i) stating the nature of the proposal and the reasons for that proposal, and
- (ii) giving the operator an opportunity to make representations in writing to the competent authority in respect of the proposal within 15 working days of the date of the notification of the proposal.

(5) The competent authority shall consider any representations made by the operator of essential services in accordance with paragraph (4) and shall, within 20 working days of the earlier of—

- (a) the receipt of the representations, or
- (b) the expiration of the period referred to in that paragraph,

decide whether to make the cancellation.

(6) Where a competent authority decides to make the cancellation, it shall notify the operator of essential services concerned in writing accordingly.

(7) Where a cancellation is made, the competent authority making the cancellation shall promptly amend the Operators Register maintained by it under Regulation 16 and where the cancellation is made by the competent authority referred to in Regulation 7(2) a copy of the amended Operators Register maintained by that competent authority shall be promptly furnished to the competent authority referred to in Regulation 7(1) who shall amend the Combined Operators Register accordingly.

(8) Where a person ceases to be designated as an operator of essential services the competent authority shall, as soon as possible after such cessation, notify the person in writing accordingly.

*Register of Operators of Essential Services, Combined Operators Register*

16. (1) A competent authority shall establish and maintain a register to be known as the Register of Operators of Essential Services (in these Regulations referred to as the “Operators Register”) containing particulars of operators of essential services in each sector in respect of which the competent authority is designated as the competent authority.

(2) The Operators Register shall, in respect of a person who is an operator of essential services, contain particulars of—

- (a) the person, and
- (b) the category of sector and, as appropriate, subsector and the essential service in respect of which the person is an operator of essential services.

(3) The competent authority shall—

- (a) review the Operators Register established by it on a regular basis and, in any event, not less than once in every two years from 9 May 2018, and
- (b) amend the Operators Register established by it in accordance with Regulations 14 and 15.

(4) A copy of the Operators Register established by the competent authority referred to in Regulation 7(2) shall be furnished by it to the competent authority referred to in Regulation 7(1) as soon as possible after it has been established.

(5) The competent authority referred to in Regulation 7(1) shall establish a Combined Operators Register which comprises the Operators Register established by that competent authority and the Operators Register furnished to it under paragraph (4) by the competent authority referred to in Regulation 7(2), as may be amended from time to time in accordance with Regulations 14 and 15.

*Security requirements in respect of operators of essential services*

17. (1) An operator of essential services shall—

- (a) take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems which it uses in its operations, and
- (b) take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used by it for the provision of the essential services in respect of which it is designated as an operator of essential services with a view to ensuring the continuity of the provision by it of those services.

(2) The measures to be taken by an operator of essential services pursuant to paragraph (1) shall ensure, having regard to the state of the art, a level of security of network and information systems appropriate to the risks posed.

*Incident notification by operators of essential services*

18. (1) (a) An operator of essential services shall notify the CSIRT in accordance with paragraph (2) of any incident concerning it that has a significant impact on the continuity of an essential service provided by it in respect of which it is designated as an operator of essential services.

- (b) An operator of essential services who relies on a third-party digital service provider for the provision of an essential service in respect of which it is designated as an operator of essential services shall notify the CSIRT in accordance with paragraph (2) of an incident affecting the digital service provider which has a significant impact on the continuity of the essential service provided by the operator.

(2) A notification in respect of an incident shall be made under paragraph (1) without delay after the incident occurs and, in any event, not later than 72 hours after the operator of essential services concerned becomes aware of the occurrence of that incident.

(3) A notification made under paragraph (1) shall, to the extent to which the operator concerned may reasonably be expected to have such information, contain the following information:

- (a) the operator's name;
- (b) the category of sector and, where appropriate, subsector and the essential service provided by it which is affected by the incident;
- (c) the time the incident occurred;
- (d) the duration of the incident;
- (e) information concerning the nature and impact of the incident;
- (f) information concerning any or any likely cross-border impact of the incident;
- (g) any other information that may be of assistance to the CSIRT.

(4) In determining whether, in relation to an incident affecting an essential service provided by an operator of essential services and in respect of which the operator is designated as an operator of essential services, the incident has a significant impact on the continuity of the essential service, the following in particular shall be taken into account:

- (a) the number of users affected by the disruption of the essential service;
- (b) the duration of the incident;
- (c) the geographical spread of the area affected by the incident.

(5) The CSIRT shall without delay furnish a copy of a notification made to it under paragraph (1) to the single point of contact and the competent authority referred to in Regulation 7(1) and, where the notification relates to an incident in a sector referred to in Regulation 7(2), a copy of the notification shall also be furnished without delay to the competent authority referred to in that Regulation.

- (6) (a) The CSIRT shall, where it is satisfied that an incident notified to it may have a significant impact on the continuity of the provision of an essential service in another member state having regard to the matters referred to in paragraph (4), inform the single point of contact in the other member state of the incident and may request the single point of contact to forward the notification made under paragraph (1) to the single point of contact in the other member state.
- (b) Where requested to do so by the CSIRT or a competent authority, the single point of contact shall send the notification to the single point of contact in the other member state.

(7) Where possible, the CSIRT shall provide an operator of essential services who has made a notification under this Regulation with information in relation to dealing with the incident to which the notification relates, including information that may assist the operator in effective incident handling.

(8) After consulting with the operator of essential services to whom a notification under paragraph (1) relates and, where the notification relates to an incident in a sector referred to in Regulation 7(2) with the competent authority referred to in that Regulation, the CSIRT may inform the public about the incident to which the notification relates where the CSIRT considers that public awareness is necessary to deal with the incident insofar as it relates to the operator of essential services concerned or to prevent the same or a similar incident occurring in respect of other operators of essential services who the CSIRT considers may be at risk of such an incident having regard to the nature of the incident and the network and information systems of those other operators.

(9) An operator of essential services that has made a notification under paragraph (1) shall notify the CSIRT in accordance with paragraph (10) when the incident has been resolved.

(10) A notification under paragraph (9) shall be made as soon as practicable after the incident has been resolved and, in any event, not later than 72 hours after that time.

(11) The CSIRT shall without delay furnish a copy of a notification made under paragraph (9) to a person to whom a copy of the notification made under paragraph (1) was furnished under paragraph (5).

(12) The CSIRT shall without delay forward a copy of any correspondence between it and an operator of essential services in relation to an incident notified to it under paragraph (1) to—

- (a) the competent authority referred to in Regulation 7(1), and
- (b) where the incident relates to a sector referred to in Regulation 7(2), the competent authority referred to in that Regulation.

(13) A notification made under this Regulation shall be in such form and manner as the competent authority referred to in Regulation 7(1) shall determine.

(14) An operator of essential services commits an offence where it does not notify the CSIRT in accordance with paragraph (1) or (9).

(15) In a prosecution for an offence under paragraph (14) it shall be a defence for an operator of essential services to show—

- (a) that the operator took all reasonable steps to notify the CSIRT in accordance with paragraph (1) or (9), as the case may be, or

- (b) it was not reasonably possible for the operator to notify the CSIRT in accordance with paragraph (1) or (9), as the case may be.

## PART 5

### DIGITAL SERVICES

#### *Definition*

19. In this Part, “digital service” means a digital service set out in Schedule 2 which is normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services where—

“at a distance” in relation to a digital service means that the service is provided without the party providing the service and the party receiving the service being simultaneously present,

“by electronic means” in relation to a digital service means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,

and

“at the individual request of a recipient of services” in relation to a digital service means that the service is provided through the transmission of data on individual request.

#### *Relevant digital service provider*

20. (1) A relevant digital service provider means a digital service provider who, in respect of a digital service—

- (a) provides the digital service in the Union,
- (b) has its main establishment in the State or has designated a representative in the State, and
- (c) is not a micro or small enterprise as defined in Commission Recommendation 2003/361/EC of 6 May 2003<sup>6</sup> concerning the definition of micro, small and medium-sized enterprises.

(2) Where a relevant digital service provider is—

- (a) an undertaking which is subject to the requirements of Regulations 23 and 24 of the European Communities (Electronic Communications Network and Services) (Framework) Regulations 2011, or
- (b) a trust service provider subject to the requirements of Article 19 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014,

<sup>6</sup>O.J. No. L 124, 20.5.2003, p.36

these Regulations apply to the relevant digital service provider in respect only of any digital service provided by it.

(3) A digital service provider is deemed to have its main establishment in the State where its head office is in the State.

*Security measures to be taken by relevant digital service providers*

21. (1) A relevant digital service provider shall identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems used by it when offering a service set out in Schedule 2 in the Union.

(2) The measures to be taken under paragraph (1) shall, having regard to the state of the art—

- (a) ensure a level of security of network and information systems appropriate to the risk posed, and
- (b) take into account the following in accordance with the Implementing Regulation:
  - (i) the security of systems and facilities;
  - (ii) incident handling;
  - (iii) business continuity management;
  - (iv) monitoring, auditing and testing;
  - (v) compliance with international standards.

(3) A relevant digital service provider shall take measures to prevent and minimise the impact of incidents affecting the security of its network and information systems on a service set out in Schedule 2 that is offered by it within the Union with a view to ensuring the continuity of the provision by it of that service.

(4) A relevant digital service provider shall ensure that it has sufficient documentation to enable the competent authority to verify the compliance by the relevant digital service provider with the security requirements provided for in this Regulation.

*Incident notification by a relevant digital service provider*

22. (1) A relevant digital service provider shall notify the CSIRT in accordance with paragraph (3) of any incident that has a substantial impact on the provision by it of a digital service set out in Schedule 2 which is offered by it within the Union.

(2) Paragraph (1) shall not apply where a relevant digital service provider does not have access to the information required to assess the impact of an incident taking into account the matters referred to in paragraph (4).



(3) A notification shall be made under paragraph (1) as soon as practicable after an incident occurs and, in any event, shall be made not later than 72 hours after the relevant digital service provider becomes aware of the occurrence of the incident.

(4) In determining whether to notify an incident under paragraph (1), a relevant digital service provider shall—

(a) shall take into account the following in accordance with the Implementing Regulation:

- (i) the number of users affected by the disruption of the essential service;
- (ii) the duration of the incident;
- (iii) the geographical spread of the area affected by the incident;
- (iv) the extent of the disruption of the functioning of the service;
- (v) the extent of the impact of the incident on economic and societal activities,

and

(b) assess whether a situation referred to in Article 4 of the Implementing Regulation has occurred.

(5) A notification under this Regulation shall include—

- (i) the name of the relevant digital service provider,
- (ii) details of when the incident occurred,
- (iii) the duration of the incident,
- (iv) sufficient information to enable the CSIRT to determine whether the incident has any impact on another member state, and, if so, its significance, and
- (v) any other information which may be of benefit to the CSIRT.

(6) The CSIRT shall as soon as possible furnish a copy of a notification made to it under paragraph (1) to the single point of contact and the competent authority.

(7) Where appropriate, and in particular if an incident referred to in paragraph (1) concerns another member state, the competent authority or the CSIRT shall notify the single point of contact in the other affected member state of the incident.

(8) Where possible, the CSIRT shall provide a relevant digital service provider who has made a notification under this Regulation with information in relation to dealing with an incident, including information that may assist in effective incident handling by the relevant digital service provider concerned.

(9) After consulting the relevant digital service provider in relation to an incident relating to it, the CSIRT may inform the public or may require the relevant digital service provider to inform the public, about the incident where the CSIRT considers that public awareness is necessary to deal with the incident insofar as it relates to the relevant digital services provider concerned or to prevent the same or a similar incident occurring in respect of other relevant digital service providers who the CSIRT considers may be at risk of such an incident having regard to the nature of the incident and the network and information systems of those other relevant providers or where disclosure of the incident is otherwise in the public interest.

(10) A relevant digital service provider that has made a notification under paragraph (1) shall notify the CSIRT in accordance with paragraph (11) when the incident has been resolved.

(11) A notification under paragraph (10) shall be made as soon as practicable after the incident has been resolved and, in any event, not later than 72 hours after that time.

(12) The CSIRT shall forward a copy of the notification made under paragraph (10) and any other correspondence between it and a relevant digital service provider in relation to an incident referred to in paragraph (1) to a person to whom a copy of the notification made under paragraph (1) was furnished under paragraph (6).

(13) A notification made under this Regulation shall be such form and manner as the competent authority shall determine.

(14) A relevant digital service provider commits an offence where it does not notify the CSIRT in accordance with paragraph (1) or (10).

(15) In a prosecution for an offence under paragraph (14) it shall be a defence for a relevant digital service provider to show that—

- (i) it took all reasonable steps to notify the CSIRT in accordance with paragraph (1) or (10), as the case may be, or
- (ii) it was not reasonably possible for it to notify the CSIRT in accordance with paragraph (1) or (10), as the case may be.

*Co-operation and assistance in respect of relevant digital service providers whose network and information systems are not in State*

23. (1) Where the network and information systems of a relevant digital service provider are located in one or more member states other than the State, the competent authority may, for the purpose of assessing the compliance by the relevant digital service provider with its obligations under these Regulations,

request the co-operation and assistance of the competent authority in the other member state or states.

(2) For the purpose of a request referred to in paragraph (1), the competent authority may do one or both of the following:

- (a) share information with the competent authority in the other member state in relation to the relevant digital service provider;
- (b) request the competent authority in the other member state to require the relevant digital service provider to provide to that competent authority the information necessary for the security of the provider's network and information systems to be assessed by the CSIRT.

*Co-operation in respect of digital service providers whose main establishment or designated representative not in State but whose network and information systems are in State*

24. (1) Where a digital service provider has its network and information systems in the State but has its main establishment in one or more member states other than the State or has designated a representative in a member state other than the State for the purposes of the Directive, the competent authority shall co-operate with the competent authority in the other member state in relation to the compliance by the digital service provider with its obligations under the Directive.

(2) The co-operation and assistance referred to in paragraph (1) may include one or more of the following:

- (a) the sharing of information with the competent authority in the other member state in relation to the digital service provider;
- (b) the consideration by the competent authority of any request made to it by the competent authority in the other member state to require the digital service provider to provide the competent authority with the information necessary for the security of the provider's network and information systems to be assessed by a relevant authority in the other member state, and
- (c) the appointment of one or more authorised officers for the purpose of this Regulation where the competent authority, having considered a request referred to in subparagraph (b), considers it appropriate to do so.

## PART 6

### GUIDELINES

#### *Guidelines*

25. (1) For the purpose of providing practical guidance as regards compliance by operators of essential services and relevant digital service providers with their obligations under these Regulations, the Minister may, from time to time and

following consultation with such persons (if any) as he or she considers appropriate, issue guidelines.

(2) Before issuing guidelines under this Regulation, the Minister shall publish on the internet a draft of the proposed guidelines and shall give persons a period of 30 working days from the date of the publication of the draft within which to make written representations to him or her in relation to that draft.

(3) The Minister may, having considered any relevant representations received under paragraph (3), issue the guidelines with or without modification.

(4) The guidelines shall specify the date on which they are to come into operation.

(5) The Minister may, following consultation with such persons (if any) as he or she considers appropriate, amend or revoke guidelines published under this Regulation.

(6) The Minister shall publish the guidelines and, where they have been amended, the guidelines as so amended, on the internet.

## PART 7

### VOLUNTARY NOTIFICATION

#### *Voluntary Notification*

26. (1) A person who is not an operator of essential services or a relevant digital service provider may notify the CSIRT on a voluntary basis of an incident having a significant impact on the continuity of the services provided by the person.

(2) The CSIRT may prioritise dealing with notifications made under Regulations 18 and 22 over those made under this Regulation.

(3) A notification under this Regulation shall only be processed by the CSIRT where such processing does not constitute a disproportionate or undue burden on the CSIRT.

(4) A notification under this Regulation shall not result in the notifying entity being subject to any obligations to which it would not be subject had it not made the notification.

(5) The CSIRT may provide assistance to a person who makes a notification under this Regulation in relation to the handling of the incident.

## PART 8

### IMPLEMENTATION AND ENFORCEMENT

#### *Security assessment*

27. (1) (a) The competent authority referred to in Regulation 7(1) may, in relation to those sectors in respect of which it is designated as the

competent authority, carry out an assessment, whether by means of a security audit or otherwise, of the compliance by an operator of essential services with its obligations under Regulations 17 and 18 and for that purpose may appoint an independent person or auditor to carry out the assessment on its behalf.

- (b) The competent authority referred to in Regulation 8 may, in relation to a relevant digital service provider, carry out an assessment, whether by means of a security audit or otherwise, of the compliance by a relevant digital service provider with its obligations under Regulations 21 and 22 and for that purpose may appoint an independent person or auditor to carry out the assessment on its behalf.

(2) A competent authority referred to in paragraph (1) may request an operator of essential services or a relevant digital service provider, as the case may be, to provide the competent authority with—

- (a) the information necessary for that competent authority to assess the security of the network and information systems of the operator or provider, as the case may be, including documented security policies, and
- (b) evidence of the effective implementation by the operator or provider, as the case may be, of security policies including the implementation of any recommendations made on foot of a security audit or other assessment.

*Appointment of authorised officers*

28. (1) (a) The competent authority referred to in Regulation 7(1) may, in relation to those sectors in respect of which it is designated as the competent authority, appoint such and so many persons as it thinks fit to be authorised officers for the purposes of any or all of these Regulations and of ensuring compliance by operators of essential services in those sectors with their requirements.

- (b) The competent authority referred to in Regulation 8 may appoint such and so many persons as it thinks fit to be authorised officers for the purposes of any or all of these Regulations and of ensuring compliance by relevant digital service providers with their requirements or, where Regulation 24 applies, of assisting a competent authority in another member state in accordance with that Regulation.

(2) A competent authority referred to in paragraph (1) may terminate the appointment of an authorised officer appointed by the competent authority, whether or not the appointment was for a fixed period.

(3) An appointment as an authorised officer ceases—

- (a) if it is terminated under paragraph (2),
- (b) if it is for a fixed period, on the expiry of that period, or

- (c) if the person appointed is an officer of the competent authority referred to in paragraph (1), on the person ceasing to be such an officer.

(4) An authorised officer shall be furnished with a warrant of his or her appointment and shall, when exercising any power conferred on him or her under these Regulations, if requested by a person affected, produce the warrant of appointment or a copy of it to that person together with a form of personal identification.

*Powers of authorised officers*

29. (1) Other than insofar as these Regulations relate to operators of essential services in a sector referred to in Regulation 7(2), an authorised officer shall, for the purposes of any or all of these Regulations and of ensuring compliance with their requirements or, where Regulation 24 applies, of assisting a competent authority in another member state in accordance with that Regulation, have power to do any or all of the following:

- (a) subject to subparagraph (d), at all reasonable times enter and examine any place owned or operated by—
  - (i) an operator of essential services,
  - (ii) a relevant digital service provider,
  - (iii) a digital service provider referred to in Regulation 24, or
  - (iv) a person on behalf of a person referred to in clause (i), (ii) or (iii),
 for the purpose of—
  - (I) in relation to an operator of essential services or a relevant digital service provider, assessing the compliance by that operator or provider with its obligations under these Regulations and the effects of such compliance on the security of its network and information systems, or
  - (II) in relation to a digital service provider referred to in clause (iii), assisting a competent authority in another member state under Regulation 24,

and for those purposes to search and inspect the place, any process being carried out and any books, documents or records or things found at that place to the extent to which the place, process, books, documents or records or things relate to the network and information systems of that operator or provider;

- (b) at a place referred to in subparagraph (a), request, inspect, review and examine any books, documents or records in respect of the security of network and information systems of a person referred to in subparagraphs (a)(i) to (iii) which the authorised officer may reasonably

require for the purpose of any search, examination, investigation, inspection, assessment or inquiry under these Regulations including, but not limited to, books, documents or records relating to the certification of the security and technical specifications of the systems and the implementation of the recommendations of any security audit in respect of those systems;

- (c) require any person in charge of, or employed in, a place referred to in subparagraph (a) to produce to the authorised officer such books, documents or records (and in the case of such information in a non-legible form to reproduce it in a permanent legible form) that are in the person's power, possession or control or to give to the authorised officer such information as the officer may reasonably require in relation to any entries in such books, documents or records;
- (d) to inspect and take copies of or extracts from any such books, documents or records (including in the case of information in non-legible form a copy of or an extract from such information in a permanent legible form) or require that such a copy be provided;
- (e) interview any person whom the authorised officer reasonably believes to be able to give to the authorised officer information or records relevant to any search, examination, investigation, inspection, assessment or inquiry under these Regulations and require the person to answer such questions as the authorised officer may ask relative to the search, examination, investigation, inspection, assessment or inquiry and to sign a declaration of the truth of the answers;
- (f) require any person to afford the authorised officer such facilities and assistance within the person's power, control or responsibilities as are reasonably necessary to enable the authorised officer to exercise any of the powers conferred on him or her by these Regulations.

(2) When performing a function under these Regulations, an authorised officer may, subject to any warrant under paragraph (5), be accompanied by such number of authorised officers or members of the Garda Síochána as he or she considers appropriate.

(3) An authorised officer shall not, other than with the consent of the occupier, enter a private dwelling unless he or she has obtained a warrant from the District Court under paragraph (5) authorising such entry.

(4) Where an authorised officer in the exercise of his or her powers under this Regulation is prevented from entering any place, an application may be made to the District Court under paragraph (5) for a warrant authorising such entry.

(5) If a judge of the District Court is satisfied on the sworn information of an authorised officer that there are reasonable grounds for suspecting that there is information required by an authorised officer under this Regulation held in any place or any part thereof, or that there is a record or thing which an authorised

officer requires to inspect for the purposes of these Regulations, and that such inspection is likely to disclose evidence of a contravention of these Regulations, the judge may issue a warrant authorising an authorised officer, accompanied by such other authorised officers or members of the Garda Síochána as may be necessary at any time or times within one month from the date of issue of the warrant, on production of the warrant, if requested, to enter the place, if necessary by reasonable force, and perform the functions or exercise all or any of the powers conferred on an authorised officer under these Regulations.

(6) An application under paragraph (5) shall be made to the judge of the District Court in whose District Court district the place is situated.

(7) A person shall not—

- (a) obstruct or interfere with an authorised officer or a member of the Garda Síochána in the exercise of the powers conferred on him or her by these Regulations or a warrant under paragraph (5),
- (b) without reasonable excuse fail or refuse to comply with a request from or requirement of or to answer a question asked by an authorised officer or such member pursuant to a power conferred by these Regulations, or
- (c) make a statement or give information to an authorised officer or such member that the person knows is false or misleading in a material respect.

(8) A statement or admission made by a person pursuant to a requirement under paragraph (1) (c) or (e) shall not be admissible in proceedings brought against that person for an offence (other than an offence under paragraph (9)).

(9) A person who contravenes paragraph (7) is guilty of an offence.

(10) A person who falsely represents himself or herself to be an authorised officer is guilty of an offence.

(11) A person who prevents any person from answering any question to which an authorised officer may require an answer under this Regulation commits an offence.

(12) A person who fails to comply with a bona fide request, instruction or direction from an authorised officer in the exercise of his or her functions under this Regulation, commits an offence.

(13) In this Regulation—

“place” means any structure, premises, land or other location or part of such place, and includes any container, railway wagon, vessel, aircraft, motor or other vehicle;

“person in charge”, in relation to a place, means—



- (i) the person under whose direction and control the activities at that place are being conducted, or
- (ii) the person whom the authorised officer has reasonable grounds for believing is in control of that place;

“record” includes any memorandum, book, report, statement, register, plan, chart, map, drawing, specification, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (including data that constitute personal data) are held, any form (including machine-readable form) or thing in which information is held or stored manually, mechanically or electronically, and anything that is a part or copy, in any form, of any of, or any combination of, the foregoing.

*Compliance notice*

30. (1) In this Regulation, “appeal” means an appeal under paragraph (8).

(2) Where an authorised officer is of the opinion that a provision of these Regulations is not being or has not been complied with by an operator of essential services or a relevant digital service provider the authorised officer may serve a notice (referred to in these Regulations as a “compliance notice”) on that operator or provider.

(3) A compliance notice—

- (a) shall state that the authorised officer is of the opinion referred to in paragraph (2),
- (b) shall state the reason for the opinion of the authorised officer referred to in paragraph (2),
- (c) shall identify the provision of these Regulations in respect of which that opinion is held,
- (d) shall require the person on whom it is served to take such action as is specified in the notice to remedy the non-compliance or suspected non-compliance,
- (e) may require that the person provide the authorised officer with information at such intervals as are specified in the notice in relation to the progress made in remedying the non-compliance or suspected non-compliance,
- (f) shall inform the person of the requirement to confirm compliance with the notice as referred to in paragraph (6),
- (g) shall inform the person of the right to appeal the notice and the requirements of paragraph (9),
- (h) shall include an address for service of an appeal,

- (i) shall be signed and dated by the authorised officer, and
  - (j) shall state that if the person on whom it is served fails to comply with the notice, the person commits an offence and shall be liable on conviction to the penalty referred to in Regulation 34.
- (4) (a) Subject to subparagraph (b), a compliance notice shall be complied with within such period as may be specified in the notice which period shall not be less than 14 working days after the date of the notice.
- (b) Upon the written application of the person on whom a notice is served, the period specified in the notice as the period within which that notice must be complied with may be extended by and at the discretion of the authorised officer and, where the period is so extended, the compliance notice shall be complied with within such extended time period.
- (5) A compliance notice may include directions—
  - (a) as to the action to be taken to remedy the non-compliance to which the notice relates, and
  - (b) to bring the notice to the attention of any person who may be affected by the non-compliance or to the notice of the public generally.
- (6) A person on whom a compliance notice has been served shall confirm in writing to the authorised officer concerned that the compliance notice has been complied with as soon as practicable after so complying and in any case not later than 7 working days after the date specified in the notice by which it is to be complied with or, where the period of time has been extended under paragraph (4), the date specified in accordance with the extension.
- (7) Where a person on whom a compliance notice has been served so confirms in writing under paragraph (6) that the compliance notice has been complied with, the authorised officer shall, on being so satisfied, not later than one month after the date of receipt of such confirmation, serve notice on the person concerned of compliance with the compliance notice.
- (8) A person aggrieved by a compliance notice may, not later than 14 working days after the date on which the notice is served on the person, appeal against the notice to a judge of the Circuit Court for the circuit in which the notice was served and, in determining the appeal, the judge may, if he or she is satisfied that it is reasonable to do so, confirm, vary or cancel the notice.
- (9) Notice of an appeal shall contain a statement of the grounds upon which the appeal is made and shall be lodged by the appellant with the appropriate office of the Circuit Court not later than 14 working days after the date upon which the compliance notice was served on the appellant.
- (10) A copy of the notice by which a person makes an appeal shall be given by the appellant to the authorised officer not later than 48 hours before the

hearing of the appeal and the authorised officer shall be entitled to appear, be heard and adduce evidence on the hearing of the appeal and at the hearing of any application referred to in paragraph (16).

(11) Where an appeal is made and the compliance notice is not cancelled, the person on whom the compliance notice was served shall comply with the notice by the later of—

- (a) the day immediately after the end of the period of 14 working days after the date of the determination of the appeal and the confirmation of the notice,
- (b) the date of the withdrawal of the appeal, or
- (c) the day specified in the compliance notice or, where the period of time has been extended under paragraph (4), the day specified in accordance with the extension.

(12) Where no appeal is made, the person on whom the compliance notice was served shall comply with the notice by the later of—

- (a) the day immediately after the end of the period within which an appeal may be made, or
- (b) the day specified in the compliance notice or, where the period of time has been extended under paragraph (4), the day specified in accordance with the extension.

(13) An authorised officer may, where he or she considers it appropriate to do so, by notice in writing to the person on whom a compliance notice was served, withdraw the compliance notice.

(14) A person on whom a compliance notice is served who fails to comply with, or causes or permits another person to contravene, the notice is guilty of an offence.

(15) It shall be a defence in a prosecution for an offence under paragraph (14) for a person to show—

- (i) that the person took all reasonable steps to ensure compliance with the compliance notice, or
- (ii) it was not reasonably possible for the person to comply with the notice.

(16) Where a person fails to comply with a compliance notice the authorised officer may apply to the judge of the Circuit Court for the circuit in which the notice was served for an order requiring the person to comply with the terms of the notice and the Court may make an order directing the person to comply with the notice.

- (17) A person on whom a compliance notice has been served shall not—
- (a) pending the determination of an appeal, deal with a product, place, machinery, equipment or other thing to which the notice relates, other than in accordance with the terms of the compliance notice, or
  - (b) if the notice is confirmed or varied on appeal, deal with a product, place, machinery, equipment or other thing to which the notice relates other than in accordance with the terms of the compliance notice as confirmed or varied.
- (18) A person who fails to comply with paragraph (17) is guilty of an offence.
- (19) It shall be a defence in a prosecution for an offence under paragraph (18) for a person to show—
- (i) that the person took all reasonable steps not to do the action complained of, or
  - (ii) it was not reasonably possible for the person not to do the action complained of.
- (20) This Regulation shall not operate to prevent or restrict—
- (a) the entitlement of any person to bring proceedings for the purpose of securing compliance with these Regulations, or
  - (b) the bringing or prosecuting of any proceedings for an offence under these Regulations.

*Information notice*

31. (1) A competent authority may, by notice served on a person, require the person to furnish, in writing, within such period as may be specified in the notice and, if applicable, in the format or manner specified in the notice, such information specified in the notice that the competent authority may reasonably require for the proper performance by the competent authority of its functions under these Regulations.
- (2) An information notice shall specify the purpose for which it is being served.
- (3) An information notice shall—
- (a) inform the person on whom the information notice is served that he or she may appeal against a requirement specified in the notice to the Circuit Court in accordance with this Regulation, and
  - (b) state that if the person on whom the information notice is served fails to comply with the notice, that person commits an offence.

(4) Upon the written application of the person on whom the notice is served, the period specified in the information notice may be extended by and at the discretion of the competent authority.

(5) A person on whom an information notice is served may, within 7 working days of the day on which the notice is served on the person, appeal against a requirement specified in the notice to a judge of the Circuit Court for the circuit in which the notice was served and in determining the appeal the judge may, if he or she is satisfied that it is reasonable to do so, confirm, vary or cancel the notice.

(6) A person who appeals under paragraph (5) shall at the same time notify the competent authority of the appeal and the grounds for the appeal and the competent authority shall be entitled to appear, be heard and adduce evidence on the hearing of the appeal.

(7) Where, on the hearing of an appeal under this Regulation, an information notice is confirmed or varied, the judge by whom the appeal is heard may, on the application of the appellant, suspend the operation of the notice for such period as in the circumstances of the case the judge considers appropriate.

(8) Subject to paragraph (9), a person on whom an information notice is served shall comply with the notice before—

- (a) the end of the period specified in the notice, or
- (b) where the period referred to in subparagraph (a) is extended under paragraph (4), the end of that extended period.

(9) Where an appeal is brought under this Regulation, and the information notice to which the appeal relates is confirmed or varied or the appeal is withdrawn, the person on whom the notice is served shall comply with the notice before—

- (a) the day immediately after the day on which the notice is confirmed or varied or the appeal is withdrawn,
- (b) the end of the period specified in the notice,
- (c) where the period referred to in subparagraph (b) has been extended under paragraph (4), the end of that extended period, or
- (d) where the operation of the notice has been suspended under paragraph (7), the end of the period of suspension,

whichever occurs latest.

(10) A person on whom an information notice has been served and who fails to comply with, or causes or permits another person to contravene, a provision or a requirement of this Regulation commits an offence.

(11) It shall be a defence in a prosecution for an offence under paragraph (10) for a person to show, in respect of the provision or requirement of this Regulation to which the prosecution relates—

- (i) that the person took all reasonable steps to ensure compliance with that provision or requirement, or
- (ii) that it was not reasonably possible for the person to comply with that provision or requirement.

(12) A person who, in purported compliance with a requirement in an information notice, furnishes information to the competent authority that he or she knows to be false or misleading in a material respect commits an offence.

(13) Other than where an information notice has been served on a person by the competent authority referred to in Regulation 7(2), an authorised officer may, where he or she considers it appropriate to do so, by notice in writing to the person on whom the information notice was served, withdraw that notice.

*Service of documents*

32. (1) Subject to paragraphs (2) and (3), a notice, direction, certificate or any other document that is required to be served on a person by these Regulations shall be in writing and addressed to the person concerned by name, and may be so served to the person in one or more of the following ways:

- (a) by delivering it to the person;
- (b) by leaving it at the address at which the person ordinarily resides or carries on business or, in a case in which an address for service has been given, at that address;
- (c) by sending it by post in a prepaid registered letter or any other form of recorded delivery service to the address referred to in paragraph (b);
- (d) where there is a facility for receiving the text of the notice by electronic means at the address at which the person carries on business or ordinarily resides, by transmitting the text of the notice by such means to such address, provided that the notice is also delivered in any of the other ways referred to in this paragraph;
- (e) if the address at which the person ordinarily resides cannot be ascertained by reasonable enquiry and the notice relates to a premises, by delivering it to the premises or by affixing it in a conspicuous position on or near the premises.

(2) Where a notice, direction, certificate or other document under these Regulations is to be served on a person who is the owner or occupier of land or property and the name of the person cannot be ascertained by reasonable inquiry, it may be addressed to the person by using the words “the owner” or, as the case may require, “the occupier”.

(3) For the purposes of this Regulation, a company formed and registered under the Companies Act 2014 (No. 38 of 2014) or an existing company within the meaning of that Act shall be deemed to be ordinarily resident at its registered office, and every other body corporate and every unincorporated body shall be deemed to be ordinarily resident at its principal office or place of business.

(4) Where an opinion, finding, statement or decision of a competent authority is contained in a document which—

- (a) purports to have been made by or at the direction of that competent authority, and
- (b) is produced in evidence by an officer of the competent authority or by an authorised officer in any proceedings,

such document shall be admissible in evidence and shall be evidence of any such opinion, finding, statement or decision in such proceedings without further proof.

#### *Offence by body corporate*

33. (1) Where an offence under these Regulations is committed by a body corporate and is proved to have been so committed with the consent or connivance of, or to be attributable to any wilful neglect on the part of, any person, being a director, manager, secretary or other officer of the body corporate, or a person who was purporting to act in any such capacity, that person, as well as the body corporate, is guilty of an offence and is liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.

(2) Where the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to the acts and defaults of a member in connection with his or her functions of management as if he or she were a director or manager of the body corporate.

#### *Penalties*

34. A person guilty of an offence under Regulation 18, 22, 29, 30, 31 or 33 is liable—

- (a) on summary conviction, to a class A fine, or
- (b) on conviction on indictment, to a fine not exceeding—
  - (i) in the case of an individual, €50,000, and
  - (ii) in the case of a person other than an individual, €500,000.

#### *Costs of prosecutions*

35. (1) Where a person is convicted of an offence under these Regulations, the Court shall, unless it is satisfied that there are special and substantial reasons for not doing so, order the person to pay to the prosecutor a sum equal to the

costs and expenses, measured by the court, reasonably incurred by the prosecutor in relation to the prosecution of the offence.

(2) An order for costs and expenses referred to in paragraph (1) shall be in addition to and not instead of any fine or penalty the court may impose.

*Prosecution of offences-operators of essential services*

36. (1) Summary proceedings for an offence under these Regulations committed by an operator of essential services other than an offence committed by an operator of essential services in a sector referred to in Regulation 7(2) may be brought and prosecuted by the competent authority referred to in Regulation 7(1).

(2) Summary proceedings for an offence under these Regulations committed by an operator of essential services in a sector referred to in Regulation 7(2) may be brought and prosecuted by the competent authority referred to in that Regulation.

*Prosecution of offences-relevant digital service providers*

37. Summary proceedings for an offence committed by a relevant digital service provider under these Regulations may be brought and prosecuted by the competent authority referred to in Regulation 8.

*Hearing of proceedings otherwise than in public*

38. If a Court is satisfied that it is desirable that the whole or part of proceedings relating to an application or an appeal under these Regulations be heard otherwise than in public because of the nature or the circumstances of the case or having regard to the interests of justice then the Court may make an order that the proceedings shall, in whole or part, be heard otherwise than in in public.



## SCHEDULE 1

Sector (1)	Subsector (2)	Type of person (3)
1. Energy	(a) Electricity	– Electricity undertakings within the meaning of section 2(1) of the Electricity Regulation Act 1999 (No. 23 of 1999)
		– Distribution system operators within the meaning of section 2(1) of the Electricity Regulation Act 1999
		– Transmission system operators within the meaning of section 2(1) of the Electricity Regulation Act 1999 and electricity transmission system operators within the meaning of Regulation 2 of the European Communities (Internal Market in Natural Gas and Electricity)(Amendment) Regulations 2015 (S.I. No. 16 of 2015)
	(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 of 13 July 2009 <sup>7</sup>
		– Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 <sup>7</sup>
		– Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 <sup>7</sup>
		– Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 <sup>7</sup>
		– LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 <sup>7</sup>
		– Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 <sup>7</sup>
		– 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 of 11 March 2008 <sup>8</sup>

<sup>7</sup>O.J. No. L 211, 14.08.2009, p.94<sup>8</sup>O.J. No. L 97, 9.4.2008, p.72

Sector (1)	Subsector (2)	Type of person (3)
		<ul style="list-style-type: none"> <li>– Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009<sup>9</sup>, 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 of 11 December 2013<sup>10</sup>, and entities operating ancillary installations contained within airports</li> <li>– 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 of 10 March 2004<sup>11</sup></li> </ul>
	(b) Rail transport	<ul style="list-style-type: none"> <li>– Infrastructure managers within the meaning of Regulation 2(1) of the European Union (Regulation of Railways) Regulations 2015 (S.I. No. 249 of 2015)</li> <li>– Railway undertakings within the meaning of Regulation 2(1) of the European Union (Regulation of Railways) Regulations 2015, including operators of service facilities within the meaning of that Regulation</li> </ul>
	(c) Water transport	<ul style="list-style-type: none"> <li>– 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 of 31 March 2004<sup>12</sup>, not including the individual vessels operated by those companies</li> <li>– Managing bodies of ports within the meaning of Regulation 2(1) of the European Communities (Port Security) Regulations 2007 (S.I. No. 284 of 2007), including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No. 725/2004 of the European Parliament and of the Council of 31 March 2004<sup>12</sup>, and entities operating works and equipment contained within ports</li> <li>– 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 of 27 June 2002<sup>13</sup></li> </ul>

<sup>9</sup>O.J. No. L 70,14.3.2009, p.11

<sup>10</sup>O.J. No. L 348, 20.12.2013, p. 1

<sup>11</sup>O.J. No. L 96, 31.3.2004, p.1

<sup>12</sup>O.J. No. L 129, 29.4.2004, p.6

<sup>13</sup>O.J. No. L 208, 5.8.2002, p. 10

Sector (1)	Subsector (2)	Type of person (3)
	(d) Road transport	<ul style="list-style-type: none"> <li>– Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014<sup>14</sup></li> <li>– 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 of 7 July 2010<sup>15</sup></li> </ul>
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 of 26 June 2013 <sup>16</sup>
4. Financial market infrastructures		<ul style="list-style-type: none"> <li>– Operators of trading venues within the meaning of Regulation 3(1) of the European Union (Markets in Financial Instruments) Regulations 2017 (S.I. No. 375 of 2017)</li> <li>– 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 of 4 July 2012<sup>17</sup></li> </ul>
5. Health sector	Health care settings (including hospitals and private clinics)	Healthcare providers as defined in Regulation 3 of the European Union (Application of Patients' Rights in Cross-Border Healthcare) Regulations 2014 (S.I. No. 203 of 2014)
6. Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption within the meaning of Regulation 3(1) of the European Communities (Drinking Water) Regulations 2014 (S.I. No. 122 of 2014) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services
7. Digital Infrastructure		<ul style="list-style-type: none"> <li>- IXPs</li> <li>- DNS service providers</li> <li>- TLD name registries</li> </ul>

<sup>14</sup>O.J. No. L 157, 23.6.2015, p.21

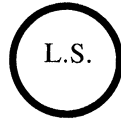
<sup>15</sup>O.J. No. L 207, 6.8.2010, p.1

<sup>16</sup>O.J. No. L 176, 27.6.2013, p. 1

<sup>17</sup>O.J. No. L 201, 27.7.2012, p.1

SCHEDULE 2

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



GIVEN under my Official Seal,  
18 September 2018.

DENIS NAUGHTEN,  
Minister for Communications, Climate Action and  
Environment.

BAILE ÁTHA CLIATH  
ARNA FHOILSIÚ AG OIFIG AN tSOLÁTHAIR  
Le ceannach díreach ó  
FOILSEACHÁIN RIALTAIS,  
52 FAICHE STIABHNA, BAILE ÁTHA CLIATH 2  
(Teil: 01 - 6476834 nó 1890 213434; Fax: 01 - 6476843)  
nó trí aon díoltóir leabhar.

---

DUBLIN  
PUBLISHED BY THE STATIONERY OFFICE  
To be purchased from  
GOVERNMENT PUBLICATIONS,  
52 ST. STEPHEN'S GREEN, DUBLIN 2.  
(Tel: 01 - 6476834 or 1890 213434; Fax: 01 - 6476843)  
or through any bookseller.

---

€8.89



Wt. (B33733). 285. 9/18. Essentra. Gr 30-15.