STATUTORY INSTRUMENTS

2022 No. 933

ELECTRONIC COMMUNICATIONS

The Electronic Communications (Security Measures) Regulations 2022

Made - - - -	*1st September 2022*
Laid before Parliament	*5th September 2022*
Coming into force - -	*1st October 2022*

The Secretary of State makes these Regulations in exercise of the powers conferred by sections 105B, 105D and 402(3) of the Communications Act 2003(**1**).

Citation, commencement and extent

1.—(1) These Regulations may be cited as the Electronic Communications (Security Measures) Regulations 2022.

(2) These Regulations come into force on 1st October 2022.

(3) These Regulations extend to England and Wales, Scotland and Northern Ireland.

Commencement Information

I1 Reg. 1 in force at 1.10.2022, see **reg. 1(2)**

Interpretation

2. In these Regulations—

"the Act" means the Communications Act 2003;

"assessed security risk", in relation to a public electronic communications network or a public electronic communications service, means the extent of the overall risk of security compromises occurring in relation to the network or service, as determined by an assessment under regulation 11(b);

"connected security compromise" has the same meaning as in section 105A of the Act(**2**);

(**1**) 2003 c. 21. Section 105B was inserted by S.I. 2011/1210 and substituted by section 1 of the Telecommunications (Security) Act 2021 (c. 31); section 105D was inserted by section 2 of that Act.

(**2**) Section 105A was inserted by S.I. 2011/1210 and substituted by section 1 of the Telecommunications (Security) Act 2021.

"content", in relation to a signal, means any element of the signal, or any data attached to or logically associated with the signal, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

(a) any meaning arising from the fact of the signal or from any data relating to the transmission of the signal is to be disregarded, and

(b) anything which is systems data as defined by section 263(4) of the Investigatory Powers Act 2016(**3**) is not content;

"incoming signal", in relation to a public electronic communications network, means any signal received by the network;

"network provider" means a person who provides a public electronic communications network;

"security critical function", in relation to a public electronic communications network or a public electronic communications service, means any function of the network or service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it;

"security permission", in relation to a public electronic communications network or a public electronic communications service, means a permission given to a person in relation to the network or service that would give the person an opportunity to cause a security compromise to occur in relation to the network or service;

"sensitive data", in relation to a public electronic communications network or a public electronic communications service, means—

(a) data which controls, or significantly contributes to, a security critical function, or

(b) data which is the content of a signal;

"service provider" means a person who provides a public electronic communications service;

"signal" has the same meaning as in section 32 of the Act.

Commencement Information

I2 Reg. 2 in force at 1.10.2022, see **reg. 1(2)**

Network architecture

3.—(1) A network provider must take such measures as are appropriate and proportionate to ensure—

(a) except in relation to an existing part of the public electronic communications network, that the network is designed and constructed in a manner which reduces the risks of security compromises occurring,

(b) in relation to an existing part of the public electronic communications network, that the part is redesigned and developed in a manner which reduces the risks of security compromises occurring, and

(c) that the public electronic communications network is maintained in a manner which reduces the risks of security compromises occurring.

(2) For the purposes of paragraph (1), an existing part of a public electronic communications network is a part that was brought into operation before the coming into force of these Regulations.

(3) The duty in paragraph (1) includes in particular a duty—

(**3**) 2016 c. 25.

(a) to identify and reduce the risks of security compromises to which the network as a whole and each particular function, or type of function, of the network may be exposed, having appropriate regard to the following—

(i) whether the function contains sensitive data,

(ii) whether the function is a security critical function,

(iii) the location of the equipment performing the function or storing data related to the function, and

(iv) the exposure of the function to incoming signals,

(b) to make a written record, at least once in any period of 12 months, of the risks identified under paragraph (a),

(c) to identify and record the extent to which the network is exposed to incoming signals,

(d) to design and construct the network in such a way as to ensure that security critical functions are appropriately protected and that the equipment performing those functions is appropriately located,

(e) to take such measures as are appropriate and proportionate in the procurement, configuration, management and testing of equipment to ensure the security of the equipment and functions carried out on the equipment, and

(f) to take such measures as are appropriate and proportionate to ensure that the network provider—

(i) is able, without reliance on persons, equipment or stored data located outside the United Kingdom, to identify the risks of security compromises occurring,

(ii) is able to identify any risk that it may become necessary to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom, and

(iii) if it should become necessary to do so, would be able to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom.

(4) A network provider must retain any record made under paragraph (3)(b) or (c) for at least 3 years.

(5) A network provider or service provider must take such measures as are appropriate and proportionate to ensure that the public electronic communications network or public electronic communications service is designed in such a way that the occurrence of a security compromise in relation to part of the network or service does not affect other parts of the network or service.

Commencement Information

I3 Reg. 3 in force at 1.10.2022, see **reg. 1(2)**

Protection of data and network functions

4.—(1) A network provider must use such technical means as are appropriate and proportionate—

(a) to protect data which is stored by electronic means and relates to the operation of the public electronic communications network, in a manner which is appropriate to the data concerned, and

(b) to protect functions of the public electronic communications network in a manner which is appropriate to the functions concerned.

(2) A service provider must use such technical means as are appropriate and proportionate—

(a) to protect data which is stored by electronic means and relates to the operation of the public electronic communications service, in a manner which is appropriate to the data concerned, and

(b) to protect functions of the public electronic communications network by means of which the public electronic communications service is provided, so far as those functions are under the control of the service provider, in a manner which is appropriate to the functions concerned.

(3) In paragraphs (1) and (2), "protect", in relation to data or functions, means protect from anything involving a risk of a security compromise occurring in relation to the public electronic communications network or public electronic communications service in question.

(4) The duties in paragraphs (1) and (2) include in particular duties to take such measures as are appropriate and proportionate—

(a) to ensure that workstations through which it is possible to make significant changes to security critical functions are not exposed—

(i) where, in the case of a public electronic communications network, the workstation is directly connected to the network, to signals that are incoming signals in relation to the network,

(ii) where, in the case of a public electronic communications service, the workstation is directly connected to the public electronic communications network by means of which the service is provided, to signals that are incoming signals in relation to that network, or

(iii) where, in either case, the workstation is operated remotely, to signals other than those that the workstation has to be capable of receiving in order to enable changes to security critical functions authorised by the network provider or service provider to be made,

(b) to monitor and reduce the risks of security compromises occurring as a result of incoming signals received in the network or, as the case may be, a network by means of which the service is provided, and

(c) to monitor and reduce the risks of security compromises occurring as a result of the characteristics of any equipment supplied to customers which is used or intended to be used as part of the network or service.

(5) A network provider must use within the public electronic communications network signals which, by encryption, reduce the risks of security compromises occurring.

(6) A service provider must—

(a) monitor and reduce the risks of security compromises relating to customers' SIM cards occurring in relation to the public electronic communications network by means of which the public electronic communications service is provided, and

(b) replace SIM cards in cases where it is appropriate to do so in order to reduce such risks.

(7) In paragraph (6), "SIM card" means a subscriber identity module or other hardware storage device intended to store an International Mobile Subscriber Identity (IMSI) and associated cryptographic material, and the reference to replacing a SIM card includes a reference to the application to a SIM card of any process which permanently replaces one IMSI and associated cryptographic material with another.

Commencement Information

I4 Reg. 4 in force at 1.10.2022, see **reg. 1(2)**

Protection of certain tools enabling monitoring or analysis

5.—(1) This regulation applies in relation to a public electronic communications network or public electronic communications service if the network or service includes tools that enable—

(a) the monitoring or analysis in real time of the use or operation of the network or service, or

(b) the monitoring or analysis of the content of signals.

(2) If the tools are stored on equipment located outside the United Kingdom, the network provider or service provider must take measures to identify and reduce the risks of security compromises occurring as a result of the tools being stored on equipment located outside the United Kingdom.

(3) The network provider or service provider must ensure that the tools—

(a) are not capable of being accessed from a country listed in the Schedule, and

(b) are not stored on equipment located in a country so listed.

Commencement Information
I5 Reg. 5 in force at 1.10.2022, see **reg. 1(2)**

Monitoring and analysis

6.—(1) A network provider must take such measures as are appropriate and proportionate to monitor and analyse access to security critical functions of the public electronic communications network for the purpose of identifying anomalous activity that may involve a risk of a security compromise occurring.

(2) A network provider or service provider must take such measures as are appropriate and proportionate—

(a) to monitor and analyse the operation of security critical functions of the public electronic communications network or public electronic communications service for the purpose of identifying the occurrence of any security compromise, using automated means of monitoring and analysis where possible, and

(b) to investigate any anomalous activity in relation to the network or service.

(3) The duty in paragraph (2) includes in particular a duty—

(a) to maintain a record of all access to security critical functions of the network or service, including the persons obtaining access,

(b) to identify and record all cases where a person's access to security critical functions of the network or service exceeds the person's security permission,

(c) to have in place means and procedures for producing immediate alerts of all manual amendments to security critical functions,

(d) to analyse promptly all activity relating to security critical functions of the network or service for the purpose of identifying any anomalous activity,

(e) to ensure that all data required for the purposes of a duty under paragraph (1) or sub-paragraphs (a) to (c) is held securely for at least 13 months, and

(f) to take measures to prevent activities that would restrict the monitoring and analysis required by this regulation.

(4) A network provider or service provider must record the type, location, software and hardware information and identifying information of equipment supplied by the network provider or service provider which is used or intended to be used as part of the public electronic communications network or public electronic communications service.

Commencement Information

I6 Reg. 6 in force at 1.10.2022, see **reg. 1(2)**

Supply chain

7.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service as a result of things done or omitted by third party suppliers.

(2) In this regulation, "third party supplier", in relation to a network provider or service provider, means a person who supplies, provides or makes available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

(3) The risks referred to in paragraph (1) include—

(a) those arising during the formation, existence or termination of contracts with third party suppliers, and

(b) those arising from third party suppliers with whom the network provider or service provider has a contractual relationship contracting with other persons for the supply, provision or making available of any goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

(4) A network provider or service provider ("the primary provider") must take such measures as are appropriate and proportionate—

(a) to ensure, by means of contractual arrangements, that each third party supplier—

(i) takes appropriate measures to identify the risks of security compromises occurring in relation to the primary provider's network or service as a result of the primary provider's use of goods, services or facilities supplied, provided or made available by the third party supplier, to disclose any such risks to the primary provider, and to reduce any such risks,

(ii) where the third party supplier is itself a network provider and is given access to the primary provider's network or service or to sensitive data, takes appropriate measures for the purposes mentioned in section 105A(1) of the Act, in relation to goods, services or facilities supplied, provided or made available by the third party supplier to the primary provider, which are equivalent to the measures that the primary provider is required to take in relation to the primary provider's network or service,

(iii) takes appropriate measures to enable the primary provider to monitor all activity undertaken or arranged by the third party supplier in relation to the primary provider's network or service, and

(iv) takes appropriate measures to co-operate with the primary provider in the resolution of incidents which cause or contribute to the occurrence of a security compromise in relation to the primary provider's network or service or of an increased risk of such a compromise occurring,

(b) to ensure that all network connections and data sharing with third party suppliers, or arranged by third party suppliers, are managed securely, and

(c) to have appropriate written plans to manage the termination of, and transition from, contracts with third party suppliers while maintaining the security of the network or service.

(5) A network provider must—

(a) ensure that there is in place at all times a written plan to maintain the normal operation of the public electronic communications network in the event that the supply, provision or making available of goods, services or facilities by a third party supplier is interrupted, and

(b) review that plan on a regular basis.

Commencement Information

I7 Reg. 7 in force at 1.10.2022, see **reg. 1(2)**

Prevention of unauthorised access or interference

8.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to reduce the risks of the occurrence of security compromises that consist of unauthorised access to the public electronic communications network or public electronic communications service.

(2) The duty in paragraph (1) includes in particular a duty—

(a) to ensure that persons given responsibility for the taking of measures on behalf of the network provider or service provider for the purposes mentioned in section 105A(1) of the Act ("the responsible persons") have an appropriate understanding of the operation of the network or service,

(b) to require multi-factor authentication for access to an account capable of making changes to security critical functions,

(c) to ensure that significant or manual changes to security critical functions must, before the change is made, be proposed by one person authorised by the network provider or service provider in question and approved by another person from among the responsible persons,

(d) to avoid the use of default credentials wherever possible, in particular by avoiding, as far as possible, the use of devices and services with default credentials that cannot be changed,

(e) where, despite sub-paragraph (d), default credentials have been used, to assume, for the purpose of identifying the risks of security compromises occurring, that any such default credentials are publicly available,

(f) to ensure that information which could be used to obtain unauthorised access to the network or service (whether or not stored by electronic means) is stored securely, and

(g) to carry out changes to security critical functions through automated functions where possible.

(3) A network provider must have in place, and use where appropriate, means and procedures for isolating security critical functions from signals which the provider does not believe on reasonable grounds to be safe.

(4) A network provider or service provider must limit, so far as is consistent with the maintenance and operation of the public electronic communications network or the provision of the public electronic communications service, the number of persons given security permissions and the extent of any security permissions given.

(5) A network provider or service provider must also—

(a) ensure that passwords and credentials are—

(i) managed, stored and assigned securely, and

(ii) revoked when no longer needed,

(b) take such measures as are appropriate and proportionate to ensure that each user or system authorised to access security critical functions uses a credential which identifies them individually when accessing those functions,

(c) take such measures as are appropriate and proportionate, including the avoidance of common credential creation processes, to ensure that credentials are unique and not capable of being anticipated by others,

(d) keep records of all persons who—

(i) in the case of a network provider, have access to the public electronic communications network otherwise than merely as end-users of a public electronic communications service provided by means of the network, and

(ii) in the case of a service provider, have access to the public electronic communications service otherwise then merely as end-users of the service, and

(e) limit the extent of the access to security critical functions given to a person who uses the network or service to that which is strictly necessary to enable the person to undertake the activities which the provider authorises the person to carry on.

(6) A network provider or service provider must ensure—

(a) that no security permission is given to a person while the person is in a country listed in the Schedule, and

(b) that any security permission cannot be exercised while the person to whom it is given is in a country so listed.

Commencement Information

I8 Reg. 8 in force at 1.10.2022, see **reg. 1(2)**

Preparing for remediation and recovery

9.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to prepare for the occurrence of security compromises with a view to limiting the adverse effects of security compromises and enabling the provider to recover from security compromises.

(2) The duty in paragraph (1) includes in particular a duty—

(a) to create or acquire, for the purposes mentioned in that paragraph, and to retain within the United Kingdom—

(i) an online copy of information necessary to maintain the normal operation of the public electronic communications network or public electronic communications service, and

(ii) so far as is proportionate, an offline copy of that information,

(b) to replace copies held for the purpose of sub-paragraph (a) with reasonable frequency, appropriate to the assessed security risk of the network or service, and

(c) to have means and procedures in place—

(i) for promptly identifying the occurrence of any security compromise and assessing its severity, impact and likely cause,

(ii) for promptly identifying any mitigating actions required as a result of the occurrence of any security compromise,

(iii) where the occurrence of a security compromise gives rise to the risk of a connected security compromise, for preventing the transmission of signals that give rise to that risk,

(iv) for dealing with the occurrence of a security compromise within a reasonable period appropriate to the assessed security risk of the network provider or service provider, and without creating any risk of a further security compromise occurring,

(v) for ensuring that, if the network provider or service provider is unable to take steps for the purposes of preventing any adverse effects (on the network or service or otherwise) arising from the occurrence of a security compromise within the period of 14 days beginning with the day on which it occurs, the network provider or service provider is able to prepare a written plan as to how and when the provider will take such measures,

(vi) for dealing with any unauthorised access to, or control over, security critical functions by taking action as soon as reasonably possible, and without creating any risk of a further security compromise occurring, to ensure that only authorised users have access to the network or service, and

(vii) for replacing information damaged by security compromises with the information contained in the copy referred to in sub-paragraph (a).

(3) For the purposes of paragraph (2)(a)—

(a) an "online copy" is a copy that is held on the public electronic communications network or public electronic communications service in question, and

(b) an "offline copy" is a copy that is stored in such a way that it is not exposed to signals conveyed by means of the network or service in question.

Commencement Information

I9 Reg. 9 in force at 1.10.2022, see **reg. 1(2)**

Governance

10.—(1) A network provider or service provider must ensure appropriate and proportionate management of persons given responsibility for the taking of measures on behalf of the provider for the purposes mentioned in section 105A(1) of the Act.

(2) The duty in paragraph (1) includes in particular a duty—

(a) to establish, and regularly review, the provider's policy as to measures to be taken for the purposes mentioned in section 105A(1) of the Act,

(b) to ensure that the policy includes procedures for the management of security incidents, at varying levels of severity,

(c) to have a standardised way of categorising and managing security incidents,

(d) to ensure that the policy provides channels through which risks identified by persons involved at any level in the provision of the network or service are reported to persons at an appropriate governance level,

(e) to ensure that the policy provides for a post-incident review procedure in relation to security incidents and that the procedure involves consideration of the outcome of the

review at an appropriate governance level and the use of that outcome to inform future policy, and

(f) to give a person or committee at board level (or equivalent) responsibility for—

(i) supervising the implementation of the policy, and

(ii) ensuring the effective management of persons responsible for the taking of measures for the purposes mentioned in section 105A(1) of the Act.

(3) In paragraph (2) "security incident" means an incident involving—

(a) the occurrence of a security compromise, or

(b) an increased risk of a security compromise occurring.

(4) A network provider or service provider must take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring as a result of unauthorised conduct by persons involved in the provision of the public electronic communications network or public electronic communications service.

Commencement Information

I10 Reg. 10 in force at 1.10.2022, see **reg. 1(2)**

Reviews

11. A network provider or service provider must—

(a) undertake regular reviews of the provider's security measures in relation to the public electronic communications network or public electronic communications service, taking into account relevant developments relating to the risks of security compromises occurring, and

(b) undertake at least once in any period of 12 months a review of the risks of security compromises occurring in relation to the network or service in order to produce a written assessment of the extent of the overall risk of security compromises occurring within the next 12 months, taking into account—

(i) in the case of a network provider, risks identified under regulation 3(3)(a),

(ii) risks identified under regulation 5(2),

(iii) risks identified under regulation 6(1),

(iv) risks identified under regulation 7(1),

(v) risks identified under regulation 10(4),

(vi) the results of reviews carried out in accordance with sub-paragraph (a),

(vii) the results of tests carried out in accordance with regulation 14, and

(viii) any other relevant information.

Commencement Information

I11 Reg. 11 in force at 1.10.2022, see **reg. 1(2)**

Patches and updates

12. A network provider or service provider must—

(a) where the person providing any software or equipment used for the purposes of the public electronic communications network or public electronic communications service makes available a patch or mitigation relating to the risks of security compromises occurring (including software updates and equipment replacement), take such measures as are appropriate and proportionate to deploy the patch or mitigation within such period as is appropriate in the circumstances having regard to the severity of the risk of security compromise which the patch or mitigation addresses,

(b) identify any need for a security update or equipment upgrade and implement the necessary update or upgrade within such period as is appropriate, having regard to the assessed security risk of the network provider or service provider, and

(c) arrange for any decision as to what period the network provider or service provider considers appropriate—

(i) for the purposes of sub-paragraph (a), in a case where the network provider or service provider considers in relation to a particular patch or mitigation that a period of more than 14 days beginning with the day on which the patch or mitigation becomes available is appropriate, or

(ii) for the purposes of sub-paragraph (b), in a case where there is a significant risk of a security compromise occurring,

to be taken at an appropriate governance level and recorded in writing.

Commencement Information

I12 Reg. 12 in force at 1.10.2022, see **reg. 1(2)**

Competency

13.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to ensure that persons given responsibility for the taking of measures on behalf of the provider for the purposes mentioned in section 105A(1) of the Act ("the responsible persons")—

(a) are competent to discharge that responsibility, and

(b) are given resources to enable them to do so.

(2) The duty in paragraph (1) includes in particular a duty to take such measures as are appropriate and proportionate—

(a) to ensure that the responsible persons have appropriate knowledge and skills to perform their responsibilities effectively,

(b) to ensure that the responsible persons are competent to enable the network provider or service provider to perform the provider's duties under regulation 6, and are given resources for that purpose,

(c) to ensure that the responsible persons—

(i) are competent to show appropriate understanding and appraisal of the activities of third party suppliers and of any recommendations made by third party suppliers for the purposes of identifying and reducing the risk of security compromises occurring, and

(ii) are given resources for that purpose, and

(d) where new equipment is supplied, provided or made available by a third party supplier—

(i) to ensure that the equipment is set up according to a secure configuration approved by appropriately trained security personnel, following procedures which enable it to be demonstrated that the configuration has been carried out in that way, and

(ii) to record any failure to meet recommendations of the third party supplier as to the measures that are essential to reduce the risk of security compromises occurring as a result of the way in which the equipment is set up.

(3) In paragraph (2)(c) and (d) "third party supplier" has the meaning given by regulation 7(2).

Commencement Information
I13 Reg. 13 in force at 1.10.2022, see **reg. 1(2)**

Testing

14.—(1) A network provider or service provider must at appropriate intervals carry out, or arrange for a suitable person to carry out, such tests in relation to the network or service as are appropriate and proportionate for the purpose of identifying the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service.

(2) The tests must involve simulating, so far as is possible, techniques that might be expected to be used by a person seeking to cause a security compromise.

(3) The network provider or service provider must ensure, so far as is reasonably practicable—

(a) that the manner in which the tests are to be carried out is not made known to the persons involved in identifying and responding to the risks of security compromises occurring in relation to the network or service or the persons supplying any equipment to be tested, and

(b) that measures are taken to prevent any of the persons mentioned in sub-paragraph (a) being able to anticipate the tests to be carried out.

(4) The references to tests in relation to the network or service include references to tests in relation to—

(a) the competence and skills of persons involved in the provision of the network or service, and

(b) the possibility of unauthorised access to places where the network provider or service provider keeps equipment used for the purposes of the network or service.

Commencement Information
I14 Reg. 14 in force at 1.10.2022, see **reg. 1(2)**

Assistance

15.—(1) Where—

(a) a security compromise occurs in relation to a public electronic communications network or public electronic communications service, and

(b) it appears to the network provider or service provider ("the relevant person") that the security compromise is one that may cause a connected security compromise in relation to another public electronic communications network or public electronic communications service,

the relevant person must, so far as is appropriate and proportionate, provide information about the security compromise to the network provider or service provider in relation to the other network or service.

(2) Information provided under paragraph (1) which relates to a particular business may not, without the consent of the person carrying on the business—

(a) be used or disclosed by the recipient otherwise than for the purpose of identifying or reducing the risk of security compromises occurring in relation to the recipient's network or service or preventing or mitigating the adverse effects of security compromises that have occurred in relation to the recipient's network or service, or

(b) be retained by the recipient any longer than is necessary for that purpose.

(3) A network provider ("provider A") must, when requested by a service provider or another network provider ("provider B"), give provider B such assistance as is appropriate and proportionate in the taking by provider B of any measure required by these Regulations in relation anything that—

(a) has occurred in relation to provider A's public electronic communications network,

(b) is a security compromise in relation to that network, and

(c) may cause a connected security compromise in relation to provider B's public electronic communications network or public electronic communications service.

(4) A service provider ("provider A") must, when requested by a network provider or another service provider ("provider B"), give provider B such assistance as is appropriate and proportionate in the taking by provider B of any measure required by these Regulations in relation to anything that—

(a) has occurred in relation to provider A's public electronic communications service,

(b) is a security compromise in relation to that service, and

(c) may cause a connected security compromise in relation to provider B's public electronic communications network or public electronic communications service.

(5) A network provider or service provider must, where necessary to reduce the risk of security compromises occurring in relation to the provider's public electronic communications network or public electronic communications service, request another person to give any assistance which paragraph (3) or (4) will require the other person to give.

Commencement Information
I15 Reg. 15 in force at 1.10.2022, see **reg. 1(2)**

Exemption for micro-entities

16.—(1) Nothing in regulations 3 to 15 applies in relation to a network provider or service provider that is a micro-entity.

(2) In the following provisions "section 384A" means section 384A of the Companies Act 2006(**4**).

(3) A network provider or service provider is a micro-entity at any time if—

(a) the network provider or service provider qualified as a micro-entity under subsection (1) or (2) of section 384A for the most recent financial year for which audited accounts are available, or

(**4**) 2006 c. 46; section 384A was inserted by S.I. 2013/3008.

(b) if audited accounts are not available, the network provider or service provider is likely to qualify, or to have qualified, as a micro-entity under subsection (1) or (2) of section 384A in relation to the first financial year for which audited accounts are expected to become available.

(4) In paragraph (3) "financial year" has the meaning given by section 390 of the Companies Act 2006.

(5) In relation to a network provider or service provider that is not a company as defined by section 1(1) of the Companies Act 2006—

(a) references in paragraph (3) and in subsections (1) to (7) of section 384A to a company's financial year are to be read as references to any period by reference to which a profit or loss account of the business of the network provider or service provider is required to be made up, and

(b) subsections (1) to (7) of section 384A are to be read with any other necessary modifications.

(6) For the purposes of this regulation, subsection (8) of section 384A—

(a) in relation to a network provider or service provider that is a limited liability partnership, is to be read as modified by regulation 5A of the Limited Liability Partnerships (Accounts and Audit) (Application of Companies Act 2006) Regulations 2008(**5**), and

(b) in relation to a network provider or service provider that is not a body corporate, is to be disregarded.

Commencement Information

I16 Reg. 16 in force at 1.10.2022, see **reg. 1(2)**

Matt Warman
Minister of State
Department for Digital, Culture, Media and Sport

(**5**) S.I. 2008/1911; regulation 5A was inserted by S.I. 2016/575.

SCHEDULE

Regulations 5(3)and 8(6)

Countries listed for purposes of regulations 5(3) and 8(6)

Commencement Information

I17 Sch. in force at 1.10.2022, see **reg. 1(2)**

Iran (Islamic Republic of Iran).

North Korea.

People's Republic of China.

Russia (Russian Federation).

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations require the providers of public electronic communications networks or public electronic communications services to take specified security measures.

Regulations 5(3) and 8(6) refer to the countries listed in the Schedule. Regulation 5(3) requires a network provider or service provider to ensure that certain tools that enable monitoring or analysis cannot be accessed from a listed country and are not stored on equipment located in a listed country. Regulation 8(6) requires a network provider or service provider to ensure that a security permission cannot be granted to, or exercised by, a person while the person is in a listed country.

Regulation 16 contains an exemption for cases where the network provider or service provider is a micro-entity as defined by that regulation.

The Regulations supplement the general duties imposed on all providers of public electronic communications networks and public electronic communications services by sections 105A and 105C of the Communications Act 2003.

A full impact assessment of the effect that this instrument will have on the costs of business, the voluntary sector and the public sector is available from the Department for Digital, Culture, Media and Sport at 100 Parliament Street London SW1A 2BQ and is published with an Explanatory Memorandum alongside this instrument on https://legislation.gov.uk.

Status:
Point in time view as at 01/10/2022.

Changes to legislation:
There are currently no known outstanding effects for the The Electronic Communications (Security Measures) Regulations 2022.