Draft Regulations laid before Parliament under paragraphs 8F(1) of Schedule 7 to the European Union (Withdrawal) Act 2018, and sections 2(6), 3(3), 6(4), 77(5) and 77(6) of the Product Security and Telecommunications Infrastructure Act 2022, for approval by resolution of each House of Parliament.

DRAFT STATUTORY INSTRUMENTS

2023 No.

CONSUMER PROTECTION

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023

Made - - - -

Coming into force - - 29th April 2024

The Secretary of State makes these Regulations in exercise of the powers conferred by section 8C of the European Union (Withdrawal) Act 2018(**1**), and by sections 1(1), 3(1), 6(1), 9(3)(b) and (6), 15(3) and 77(2) of the Product Security and Telecommunications Infrastructure Act 2022(**2**).

A draft of these Regulations has been laid before, and approved by, both Houses of Parliament in accordance with paragraph 8F(1) of Schedule 7 to the European Union (Withdrawal) Act 2018, and sections 2(6), 3(3), 6(4), 77(5) and 77(6) of the Product Security and Telecommunications Infrastructure Act 2022.

Citation, commencement and extent

1.—(1) These Regulations may be cited as the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

(2) These Regulations come into force on 29th April 2024 and extend to England and Wales, Scotland and Northern Ireland.

Interpretation

2.—(1) In these Regulations—

"defined support period" means the minimum length of time, expressed as a period of time with an end date, for which security updates will be provided;

(**1**) 2018 c. 16. Section 8C was inserted by section 21 of the European Union (Withdrawal Agreement) Act 2020 (c. 1).
(**2**) 2022 c. 46.

"ETSI EN 303 645" means the European Standard on Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645 V2.1.1 (19th June 2020))(**3**);

"hardware" means a physical electronic information system, or parts thereof, capable of processing, storing or transmitting digital data;

"ISO/IEC 29147" means the ISO/IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure standard (2nd edition, 2018)(**4**);

"manufacturer's intended purpose" means the use for which the product is intended according to the data provided by the manufacturer, including on the label, in the instructions for use, or in promotional or sales materials or statements;

"security update" means a software update that protects or enhances the security of a product, including a software update that addresses security issues which have been discovered by or reported to the manufacturer.

(2) References in these Regulations to sections, except where otherwise specified, are to sections of the Product Security and Telecommunications Infrastructure Act 2022.

Security requirements for manufacturers

3. Schedule 1 specifies security requirements that apply to manufacturers of relevant connectable products for the purposes of section 1 (power to specify security requirements).

Deemed compliance with security requirements

4. Schedule 2 specifies the conditions under which a manufacturer is to be treated as having complied with a security requirement for the purposes of section 3 (power to deem compliance with security requirements).

Multiple manufacturers

5. Where there is more than one manufacturer of a relevant connectable product, each manufacturer must meet any relevant security requirement specified in Schedule 1 or satisfy the conditions for deemed compliance in relation to that requirement in Schedule 2.

Excepted products

6. Schedule 3 specifies excepted products for the purposes of section 6 (excepted products).

Minimum information required for statement of compliance

7. Schedule 4 specifies the information that the statement of compliance must include for the purpose of section 9 (statements of compliance).

(**3**) The European Standard on Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645 V2.1.1 (19th June 2020)) is the standard set by the European Telecommunications Standards Institute for standardisation of Cyber Security for Consumer Internet of Things Products. The standard is available free of charge at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf. A copy can also be inspected free of charge by appointment by contacting the Office for Product Safety and Standards at Stanton Avenue, Teddington, Middlesex, TW11 0JZ or by email at OPSS.enquiries@beis.gov.uk.

(**4**) The ISO/IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure standard (2nd edition, 2018) is the standard set by the International Organization for standardisation, among other things, for vulnerability disclosure. A copy can be inspected free of charge by appointment by contacting the Office for Product Safety and Standards at Stanton Avenue, Teddington, Middlesex, TW11 0JZ or by email at OPSS.enquiries@beis.gov.uk.

Manufacturer retention of statement of compliance

8. Where a statement of compliance is required under section 9(2) (statements of compliance) to make a relevant connectable product available in the United Kingdom, the manufacturer of the product must retain a copy of the statement of compliance relating to the product for whichever is the longer of—

(a) a period of 10 years beginning with the date on which the statement of compliance was issued, and

(b) the defined support period for the product set out in the statement of compliance.

Importer retention of statement of compliance

9. Where a statement of compliance is required under section 15(2) (statements of compliance) to make a product available in the United Kingdom, the importer of the product must retain a copy of the statement of compliance relating to the product for whichever is the longer of—

(a) a period of 10 years beginning with the date on which the statement of compliance was issued, and

(b) the defined support period for the product set out in the statement of compliance.

Review

10.—(1) The Secretary of State must from time to time—

(a) carry out a review of the regulatory provision contained in these Regulations; and

(b) publish a report setting out the conclusions of the review.

(2) The first report must be published before the end of the period of five years beginning with the date on which these Regulations come into force.

(3) Subsequent reports must be published at intervals not exceeding five years.

Name
Minister
Department for Science, Innovation and Technology

Schedules

Schedule 1

Regulation 3

Security requirements for manufacturers

Passwords

1.—(1) The following sub-paragraphs apply to—

(a) hardware of the product when that product is not in the factory default state;

(b) software which is pre-installed on the product at the point at which the product is supplied to a customer when the product is not in the factory default state;

(c) software which is not pre-installed on the product at the point at which the product is supplied to a customer and which must be installed on the product for all manufacturer's intended purposes of the product that use—

(i) hardware;

(ii) software that is pre-installed at the point at which the product is supplied to a customer; or

(iii) software that is installable.

(2) Passwords must be—

(a) unique per product; or

(b) defined by the user of the product.

(3) Passwords which are unique per product must not be—

(a) based on incremental counters;

(b) based on or derived from publicly available information;

(c) based on or derived from unique product identifiers, such as serial numbers, unless this is done using an encryption method, or keyed hashing algorithm, that is accepted as part of good industry practice;

(d) otherwise guessable in a manner unacceptable as part of good industry practice.

(4) In this paragraph, passwords do not include—

(a) cryptographic keys;

(b) personal identification numbers used for pairing in communication protocols which do not form part of the internet protocol suite; or

(c) application programming interface keys.

(5) In this paragraph—

"application programming interface key" means a string of characters used to identify and authenticate a particular user, product, or application so that it can access the application programming interface;

"cryptographic key" means data used to encrypt and decrypt data;

"factory default state" means the state of the product after factory reset or after final production or assembly;

"good industry practice" means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced cryptographer engaged in the same type of activity;

"incremental counter" means a method of password generation in which multiple passwords are the same save for a small amount of characters which change per password to make them unique (such as 'password1' and 'password2');

"keyed hashing algorithm" means an algorithm that uses a data input ("D") and a secret key ("K") to produce a value which cannot be guessed or reproduced without knowledge of both D and K;

"secret key" means a cryptographic key intended to be known only by the person ("P") who encrypted or authorised the encrypting of the data, and any person authorised by P;

"unique per product" means unique for each individual product of a given product class or type.

Information on how to report security issues

2.—(1) The following sub-paragraphs apply to—

(a) hardware of the product;

(b) software which is pre-installed on the product at the point at which the product is supplied to a customer;

(c) software which must be installed on the product for all manufacturer's intended purposes of the product that use—

(i) hardware;

(ii) software that is pre-installed at the point at which the product is supplied to a customer; or

(iii) software that is installable;

(d) software used for, or in connection with, any manufacturer's intended purpose of the product unless the product is a smartphone or a tablet computer capable of connecting to cellular networks.

(2) The following information must be published—

(a) at least one point of contact to allow a person ("P") to report to the manufacturer security issues relating to the categories listed in sub-paragraph (1) for any of the manufacturer's relevant connectable products for which they have an obligation under section 8 (duty to comply with security requirements); and

(b) when P will receive—

(i) an acknowledgment of the receipt of a security issues report; and

(ii) status updates until the resolution of the reported security issues.

(3) The information in sub-paragraph (2) must be accessible, clear and transparent, and must be made available to P—

(a) without prior request for such information being made;

(b) in English;

(c) free of charge; and

(d) without requesting the provision of P's personal information.

Information on minimum security update periods

3.—(1) The following sub-paragraphs apply to—

(a) hardware of the product that is capable of receiving security updates;

(b) software that is capable of receiving security updates where that software is pre-installed on the product at the point at which the product is supplied to a customer;

(c) software that is capable of receiving security updates which must be installed on the product for all manufacturer's intended purposes of the product that use—

(i) hardware;

(ii) software that is pre-installed at the point at which the product is supplied to a customer; or

(iii) software that is installable;

(d) software developed by or on behalf of any manufacturer that is capable of receiving security updates and used for, or in connection with, any manufacturer's intended purpose of the product unless the product is a smartphone or a tablet computer capable of connecting to cellular networks.

(2) The defined support period must be published.

(3) If a manufacturer extends the minimum length of time for which security updates will be provided, creating a new defined support period, the new defined support must be published as soon as is practicable.

(4) The information in sub-paragraphs (2) and (3) must be accessible, clear and transparent, and must be made available to a person ("P")—

(a) without prior request for such information being made;

(b) in English;

(c) free of charge;

(d) without requesting the provision of P's personal information; and

(e) in such a way that is understandable by a reader without prior technical knowledge.

(5) Where a manufacturer publishes an invitation to purchase a relevant connectable product on its own website or on a non-paid for website under its control that contains information described in regulation 6(4)(a) of the 2008 Regulations, the information in sub-paragraphs (2) and (3) must be published alongside or otherwise given equal prominence to the information described in that regulation.

(6) The security requirements in this paragraph are not met if the defined support period is shortened after the publication of the information in sub-paragraph (2).

(7) In this paragraph—

"the 2008 Regulations" means the Consumer Protection from Unfair Trading Regulations 2008(**5**);

"invitation to purchase" has the meaning given in regulation 2(1) of the 2008 Regulations.

(**5**) S.I. 2008/1277.

Schedule 2

Regulation 4

Conditions for Deemed Compliance with Security Requirements

Passwords

1.—(1) A manufacturer is to be treated as complying with the security requirement at paragraph 1 of Schedule 1 where the condition in sub-paragraph (2) is met.

(2) The condition is that the manufacturer complies with provision 5.1-1 of ETSI EN 303 645 and, where relevant, provision 5.1-2 of ETSI EN 303 645 as if those provisions apply to the categories of hardware and software specified in paragraph 1(1) of Schedule 1.

Information on how to report security issues

2.—(1) A manufacturer is to be treated as complying with the security requirement at paragraph 2 of Schedule 1 where the condition in sub-paragraph (2) is met.

(2) The condition is that the manufacturer complies with—

(a) provision 5.2-1 of ETSI EN 303 645; or

(b) subject to sub-paragraphs (3) and (4), the following paragraphs of ISO/IEC 29147—

(i) paragraph 6.2.2;

(ii) paragraph 6.2.5; and

(iii) paragraph 6.5

as if the provision of ETSI EN 303 645 or the paragraphs of ISO/IEC29147 apply to the categories of hardware and software specified in paragraph 2(1) of Schedule 1.

(3) A manufacturer is required to publish information as to—

(a) how a person may access the mechanism for the manufacturer to receive reports described in paragraph 6.2.2 of ISO/IEC 29147;

(b) when a person making a vulnerability report will receive an acknowledgement of receipt of a report described in paragraph 6.2.5 of ISO/IEC 29147; and

(c) when a person making a vulnerability report will receive ongoing communication as described in paragraph 6.5 of ISO/IEC 29147

(4) The information at sub-paragraph (3) must be accessible, clear and transparent, and must be made available to a person ("P")—

(a) without prior request for such information being made;

(b) in English;

(c) free of charge; and

(d) without requesting the provision of P's personal information.

Information on minimum security update periods

3.—(1) A manufacturer is to be treated as complying with the security requirement at paragraph 3 of Schedule 1 where the condition in sub-paragraph (2) is met.

(2) The condition is that, subject to sub-paragraphs (3), (5) and (6) of paragraph 3 of Schedule 1 and to sub-paragraphs (3) and (4), the manufacturer complies with provision 5.3-13 of ETSI EN 303 645 as if that provision applies to the categories of hardware and software specified in paragraph 3(1) of Schedule 1.

(3) References at provision 5.3-13 of ETSI EN 303 645 to "defined support period" are to be construed in accordance with the definition in regulation 2.

(4) Reference at provision 5.3-13 of ETSI EN 303 645 to the information being published in an accessible way that is clear and transparent includes making the information available to a person ("P")—

(a) without prior request for such information being made;

(b) in English;

(c) free of charge;

(d) without requesting the provision of P's personal information; and

(e) in such a way that is understandable by a reader without prior technical knowledge.

Schedule 3

Regulation 6

Excepted connectable products

Products made available to be supplied in Northern Ireland

1.—(1) Products are excepted under this paragraph if they are products to which relevant legislation applies and are made available for supply in Northern Ireland.

(2) For the purposes of this paragraph, "relevant legislation" means legislation that is—

(a) listed in Annex 2 to the Windsor Framework; and

(b) subject to sub-paragraph (3), contains a free movement article.

(3) Where the free movement article allows, for reasons not relating to aspects covered by the relevant legislation, Member States to prohibit, restrict, or impede the making available of the product where the product complies with the relevant legislation, that legislation must also address aspects covered by Schedule 1.

(4) In this paragraph—

"free movement article" means an article that does not permit Member States to prohibit, restrict, or impede the making available of the product where the product complies with that legislation;

"Windsor Framework" has the same meaning as in Joint Declaration No. 1/2023 of the EU and the United Kingdom in the Withdrawal Agreement Joint Committee of 24 March 2023.

Charge points for electric vehicles

2.—(1) Products are excepted under this paragraph if they are charge points to which the 2021 Regulations(**6**) apply.

(2) This paragraph has effect as if the 2021 Regulations extended to England and Wales, Scotland and Northern Ireland.

(3) For the purposes of this paragraph, the references to "Great Britain" in regulation 3(2)(b) of the 2021 Regulations are to be read as if they were references to "the United Kingdom".

(4) In this paragraph—

"the 2021 Regulations" mean the Electric Vehicles (Smart Charge Points) Regulations 2021(**7**);

(**6**) S.I. 2021/1467.
(**7**) S.I. 2021/1467.

"charge point" has the meaning given in section 9(1) of the Automated and Electric Vehicles Act 2018(**8**).

Medical devices

3.—(1) Products are excepted under this paragraph if they are products to which the Medical Devices Regulations 2002(**9**) apply.

(2) But a relevant connectable product on which software to which those Regulations apply is installed or operable is not an excepted product under this paragraph.

Smart meter products

4.—(1) Products are excepted under this paragraph if they are products—

(a) supplied or installed by or on behalf of a person acting in their capacity as a licence holder under—

(i) section 7AB of the Gas Act 1986(**10**) (licensing of a person providing a smart meter communication service); or

(ii) section 6 of the Electricity Act 1989(**11**) (licences authorising supply, etc.); and

(b) that have been successfully assured under an assurance scheme.

(2) In this paragraph, "assurance scheme" means the commercial product assurance scheme administered by the National Cyber Security Centre or any other successor scheme.

Computers

5.—(1) Products are excepted under this paragraph if they are computers which are—

(a) desktop computers;

(b) laptop computers;

(c) tablet computers which do not have the capability to connect to cellular networks.

(2) But products listed in sub-paragraph (1) which, according to the manufacturer's intended purpose, are designed exclusively for children under 14 years old are not excepted products.

Schedule 4

Regulation 7

Minimum Information Required for Statements of Compliance

1.—(1) The statement of compliance must include the following information—

(a) product (type, batch);

(b) name and address of each manufacturer of the product and, where applicable, each authorised representative;

(c) a declaration that the statement of compliance is prepared by or on behalf of the manufacturer of the product;

(**8**) 2018 c. 18.
(**9**) S.I. 2002/618.
(**10**) 1986 c. 44. Section 7AB was inserted by regulation 21 of the Electricity and Gas (Smart Meters Licensable Activity) Order 2012 (S.I. 2012/2400).
(**11**) 1989 c. 29. Relevant amendments to section 6 were made by regulation 6 of the Electricity and Gas (Smart Meters Licensable Activity) Order 2012 (S.I. 2012/2400).

(d) a declaration that, in the opinion of the manufacturer, they have complied with either—

(i) the applicable security requirements in Schedule 1; or

(ii) the deemed compliance conditions in Schedule 2;

(e) the defined support period for the product that was correct when the manufacturer first supplied the product;

(f) signature, name and function of the signatory; and

(g) the place and date of issue of the statement of compliance.

(2) For the purpose of sub-paragraph (1)(d)(ii), where the reference includes conformity of a product to a specified standard or compliance by a manufacturer to a specified standard, the identification number, version and date of issue of the standard must be included in the statement of compliance where applicable.

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations create security requirements for manufacturers of relevant connectable products and set out conditions to be met for deemed compliance of a security requirement as part of the regulatory regime as set out in Part 1 of the Product Security and Telecommunications Infrastructure Act 2022 (c. 46) ("the Act").

These Regulations also set out what connectable products are excepted from the scope of the regulatory regime and further set out requirements in relation to the statement of compliance for relevant connectable products for manufacturers and importers.

Schedule 1 sets out the security requirements with which manufacturers of relevant connectable products have to comply in relation to UK consumer connectable products.

Schedule 2 sets out conditions which, if met, will deem the manufacturer compliant with the relevant corresponding security requirement.

Schedule 3 sets out the list of products to be excepted from being considered relevant connectable products for the purposes of section 4 (relevant connectable products) of the Act.

Schedule 4 sets out the minimum amount of information which is required to be stated in a statement of compliance.

A draft of these Regulations has been notified to World Trade Organisation under the United Kingdom's obligations under the Technical Barriers to Trade Agreement (notification G/TBT/N/GBR/62), as well as to the EU Commission under the Technical Standards and Regulations Directive (notification 2023/7004/XI).

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 Science, Innovation and Technology, 100 Parliament Street, London, SW1A 2BQ and is published with an Explanatory Memorandum alongside this instrument on https://www.legislation.gov.uk.