STEVENS&BOLTON

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE (SECURITY REQUIREMENTS FOR RELEVANT CONNECTABLE PRODUCTS) REGULATIONS 2023

Businesses involved in the manufacturing, importing and/or distributing of "connectable products" will now need to comply with the requirements under the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, which took effect on 29 April 2024. This is separate to and in addition to the EU Cyber Resilience Act requirements.

Broadly, the aim of the regulations is to make consumer connected products more secure against cyber attacks. Affected businesses that fail to comply can be subject to enforcement action, including potentially large fines for material compliance failures.

THE LEGISLATIVE BACKDROP

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (the Regulation) provide the detail of the security requirements indicated in the Product Security and Telecommunications Infrastructure Act 2022 (the Act).

The Act set out duties on manufacturers, importers and distributors to comply with security requirements for relevant connectable products.

Relevant connectable products are defined under the Act as either:

- A product that is capable of connecting to the internet, or
- Is capable of both sending and receiving data by means of a transmission involving electrical or electromagnetic energy, is not an internet-connectable product, and meets one of two connectability conditions set out in the Act,
- Provided the product is not an excepted product (which are set out in the Regulation), such as medical devices.

DUTIES IMPOSED

Under the Act, there are duties imposed at different levels of the supply chains.

Manufacturers, importers and distributors all have a duty to comply with security requirements (detailed in the Regulation), as well as ensuring the relevant connectable products (Products) are accompanied by a statement of compliance.

Broadly:

- **Manufacturers** have additional duties to investigate potential compliance failures, take action in relation to a compliance failure and maintain records.
- **Importers** have additional duties to not supply Products where there is a compliance failure by a manufacturer, to investigate potential compliance failures (including those of the manufacturer), take action in relation to compliance failures (including those of the manufacturer), and maintain records.
- **Distributors** have additional duties to not supply Products where there is a compliance failure by a manufacturer, and to take action for compliance failures (including those of the manufacturer).

WHAT DOES THE REGULATION ADD?

The Regulation provides the security requirements that manufacturers, importers and distributors must comply with, sets out the excepted connectable products mentioned above, and stipulates the minimum information required for statements of compliance.

The security measures implemented by the Regulation are as follows:

- **Passwords** – passwords are to be applied to the hardware and/or software of Products. Passwords must either be set by the user or be unique per Product. Where the passwords are unique per Product, there are minimum requirements for the password to ensure security.
- **Reporting security issues** – manufacturers must appoint at least one point of contact to allow a person to report security issues to the manufacturer. The manufacturer must acknowledge receipt of the report and provide status updates to the reporter.
- **Minimum security update periods** - the minimum length of time, expressed as a period of time with an end date, for which security updates will be provided must be published.

The Regulation also provides for “deemed compliance”. Manufacturers will be deemed to be complaint if they comply with certain standards such as ETSI EN 303 645 or ISO/IEC 29147.

ENFORCEMENT

The Secretary of State is responsible for enforcement under the Act. Powers include issuing compliance notices, stop notices and recall notices. It is an offence under the Act to not comply with any enforcement notice.

The Secretary of State also has the power to issues large fines up to a maximum of the greater of (i) £10m and (ii) 4% of worldwide revenue.

WHAT DO BUSINESSES NEED TO DO?

Businesses at all levels of the supply chain should consider whether the legislation applies to them and therefore, if any changes are required to their processes to ensure compliance.

EU CYBER RESILIENCE ACT

There have also been updates to EU law - the impending EU cyber resilience rules will become relevant for importers, manufacturers, and distributors of products with digital elements or so-called connected products. This follows the EU reaching an agreed position on the EU Cyber Resilience Act which is set to apply from mid-2025 for products placed on the EU market. To learn more, read our article with TEISS here.

KEY CONTACTS

For further information about any of the issues raised in this guide, please contact:

Beverley Flynn
Head of Commercial and Technology
T: +44 (0)1483 734264
M: +44 (0)7769 708486
E: beverley.flynn@stevens-bolton.com

Guy Cartwright
Managing Associate
T: +44 (0)1483 734235
M: +44 (0)7581 055083
E: guy.cartwright@stevens-bolton.com

STEVENS&BOLTON

Wey House, Farnham Road
Guildford, Surrey, GU1 4YD
Tel: +44 (0)1483 302264
Fax: +44 (0)1483 302254
DX 2423 Guildford 1
www.stevens-bolton.com

DEPARTMENTAL\60344626v1