Product Risk Radar

The Product Security and Telecommunications Infrastructure regime

Last updated: 29 November 2024

Key takeaways

- The economic loss resulting from cyber attacks is estimated at over £1 billion per year (see the Explanatory Notes to the Product Security and Telecommunications Infrastructure Act 2022 (the "**Act**")) (the Act is available here).
- The UK Product Security and Telecommunications Infrastructure regime is intended to ensure that consumer connectable devices are better protected from cyber-attacks. The new regime came into force fully from **29 April 2024**.
- Failure to comply can result in significant financial penalties (see below), so it is important to ensure that products are compliant before they are made available in the UK and that manufacturers, distributors and importers comply with their ongoing obligations in relation to those products (e.g. to notify the authorities and take corrective action in some circumstances).

What is the relevant legislation?

- The regime is made up of the Act (in this note, we focus on Part 1 of the Act rather than Part 2 which delas with telecommunications infrastructure) and the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (the "**Regulations**") (see here).
- A draft Statutory Instrument to amend the Regulations has been approved by Parliament but is not yet in force. The amendments would, for example, specify some further products which are not subject to the Product Security and Telecommunications regime, for example, certain vehicles.

What types of products does the regime apply to?

- The regime applies to a range of connected products, including smart TVs, security cameras, and alarm systems. It does not apply to used products and certain specific categories of products are excluded, such as charge points for electric vehicles, medical devices, smart meter products as well as desktops, laptops and tablets.
- Although the regime focusses on consumer protection, it can also apply to products which are supplied in a B2B context. Therefore businesses should not just assume that they do not need to comply because

they supply products to businesses rather than end consumers. For example, the Explanatory Notes to the Act include an example of the regime applying to a smart camera which is only sold to businesses but the same make and model has been made available to consumers by another distributor.

What are manufacturers, distributors and importers required to do?

- The regime sets out various requirements for manufacturers, for example:
    - a requirement to ensure that products are accompanied by a statement of compliance;
    - a requirement to comply with certain security requirements, such as password requirements and minimum security update periods (compliance can be deemed if the product complies with certain standards, such as ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements*);
    - a requirement to take all reasonable steps to investigate whether a product fails to comply with a security requirement (e.g. if a manufacturer is informed that there is or may be a compliance failure) and to maintain records of an investigation or compliance failure;
    - a requirement to notify the authorities and others in the supply chain and take corrective action if a manufacturer becomes aware or ought to be aware of a compliance failure in relation to a relevant product.
- Similar obligations apply to importers and distributors (with variations reflecting their different role in the supply chain).
- We have listed above some examples of the requirements in the regime (i.e. this is not intended to be an exhaustive description of the requirements each business must comply with to the extent that the regime applies to it).
- The Office for Product Safety and Standards ("**OPSS**") is responsible for enforcing the product security regime outlined above.

Why should businesses ensure compliance with the regime?

- The potential penalties for non-compliance are significantly higher than the fines which could generally be imposed in the UK for failure to comply with product regulatory or safety requirements. For example, penalties of £10 million or 4% of global revenues could be imposed.

The Product Security and Telecommunications Infrastructure Act 2022

Contacts

Kate Corby
Partner
London

+44 20 7919 1966
kate.corby
@bakermckenzie.com

Graham Stuart
Partner
London

+44 20 7919 1977
graham.stuart
@bakermckenzie.com

Joanne Redmond
Senior Associate
London

+44 20 7919 1067
joanne.redmond
@bakermckenzie.com

Rachel MacLeod
Senior Associate
London

+44 20 7919 1364
rachel.macleod
@bakermckenzie.com

Phoebe Bruce
Associate
London

+44 20 7919 1117
phoebe.bruce
@bakermckenzie.com

Francesca Falsini
Associate
London
+ 44 20 7919 1000
francesca.falsini
@bakermckenzie.com

Ian Walden
Of Counsel
London

+44 20 7919 1247
Ian.walden
@bakermckenzie.com