Browne Jacobson

Mandatory cybersecurity requirements for businesses in the IOT supply chain

24 May 2024

Businesses involved in the manufacture, import or distribution of consumer facing IOT devices may need to implement mandatory cybersecurity controls or face a range of penalties under the UK Product Security & Telecommunications Infrastructure (Product Security) Regime (**PTSI Regime**).

This guidance explains which businesses might be caught by the new PTSI Regime; what they need to do to comply; and the potential legal consequences if they don't meet their statutory requirements.

The PTSI Regime

The PTSI regime came into effect on 29 April 2024 and comprises two pieces of legislation:

- PTSI Act 2022; and
- PTSI (Security Requirements for Relevant Connectable Products) Regulations 2023.

Scope of the PTSI Regime

The regime applies to manufacturers (or their UK representatives), importers and distributors (**"Relevant Persons"**) of certain consumer connectable products that can connect to the internet or other networks and can transmit and receive digital data ("**Relevant Connectable Products")**. Commonly referred to as IoT or "smart" devices, Relevant Connectable Products include devices such as smartphones, smart TVs, smart speakers, connected baby monitors and connected alarm systems.

Products such as charge points for electric vehicles, medical devices and smart meter products and personal computers may be exempted from the regime. But this should always be assessed carefully as it may depend on the precise use case. For example, tablet computers that can connect to cellular networks may caught by the regime.

Compliance with the PTSI Regime

Manufacturers of Relevant Connected Products will be required to ensure, amongst other things that:

- Security requirements are met, including the use of passwords that meet prescribed standards;
- Statements of compliance are published which confirm that applicable security requirements have been met;
- Cybersecurity issues are monitored and, where appropriate, investigated, dealt with and reported on.

Importers, distributors and authorised representatives are also required to support compliance with the regime and all Relevant Persons must take reasonable steps to prevent non-compliant products being supplied to consumers.

Penalties for non-compliance

The PTSI regime gives the Secretary of State for the Department for Science, Innovation Technology (**"DSIT"**) considerable enforcement powers, including the ability to withdraw products from the market and impose fines of up to £10 million or 4% of worldwide turnover in the previous accounting year (whichever is greater).

However, the Office for Product Safety & Standards ("**OPSS**") which will act as the enforcement authority for the new regime has explained that its approach will be pragmatic, proportionate and aligned with its Enforcement Policy.

Next steps

The stated policy objective of the PTSI regime is to ensure that businesses in this space reflect good practices set out in the European Telecommunications Standards Institute (ETSI) guidelines, and the UK government's Code of Practice for consumer IoT security.

If you are involved, directly or indirectly, in the supply of IoT devices or other consumer–facing connectable products it is important that you understand whether you are in scope of the PTSI regime, and any obligations this might trigger. Depending on the maturity of your cybersecurity governance and your wider business needs this could be undertaken as a standalone piece of legal analysis or incorporate into a wider information security review.

Key contact

Francis Katamba

Partner

francis.katamba@brownejacobson.com

+44 (0)330 045 2725