Compliance and Advisory Services for the UK's PSTI Act

Connectable consumer devices in the United Kingdom are now subject to the PSTI Act.

As of 29 April 2024, buyers of connectable consumer devices in the United Kingdom (UK) will benefit from enhanced cybersecurity regulations that aim to safeguard privacy and data.

The Product Security and Telecommunications Infrastructure (PSTI) Act's product security regime is the first in the world to require basic cybersecurity protections before connected consumer products can enter the UK market for sale.

This legislation covers a wide range of popular consumer electronics featuring connectivity features, including:

- Smartphones
- Cameras, televisions and speakers
- Toys and baby monitors
- Safety products (smoke detectors, door locks, alarms, etc.)
- Home automation systems
- Appliances
- Medical devices featuring software
- Wearable trackers
- Base stations and hubs
- Tablets and laptops designed for children under 14
- Tablets with cellular connections
- Outdoor leisure products
- And other specified product categories

Exploring provisions of the PSTI Act

In an effort to make connectable consumer products less susceptible to cyberattack, the PSTI Act includes common-sense approaches to eliminate features that are known dangers.

- **Password strength** – No more universal default passwords or default passwords that are easily guessable.
- **Increased accountability** – Manufacturers must have a public point of contact where consumers can easily report vulnerabilities.
- **Greater transparency** – Manufacturers must clearly communicate to consumers regarding minimum timeframe for security updates.

Significant penalties for lack of compliance

The UK Office for Product Safety and Standards (OPSS) is tasked with enforcing the PSTI Act, including the April 2024 product security regime. The OPSS is the enforcement agency for the UK's product safety regulations, part of the Department for Business and Trade.

The PSTI Act features clear penalties to manufacturers who sell products that are not in compliance as of 29 April, 2024, such as:

- Seizure and destruction of products
- Initial fine of £10 million or more
- Fine of 4% of the manufacturer's global revenue
- Daily fines of £20,000 for ongoing breaches

How UL Solutions helps manufacturers prepare and comply with the PSTI Act

UL Solutions works closely with manufacturers to help them anticipate emerging regulations cost-effectively. We can work with you to adopt minimal EN 303 645 to demonstrate compliance with the PSTI Act and prepare for the future regulations, including the EU Radio Equipment Directives (RED).

By working with UL Solutions, manufacturers receive expert guidance from an independent provider.

Our compliance services include testing, attestation and Statements of Compliance on behalf of customers. We also offer advisory services to aid manufacturers in making a transition, including regulation digests and product lines studies, and business and logistics guidance.

Overview of Europe cybersecurity regulations

UK PSTI compliance (PSTI execution, April 29, 2024)

- **Start with the four ETSI EN 303 645 provisions:**
  - The UK PSTI regulation compliance
  - Small pilot project of ETSI EN 303 645 standards

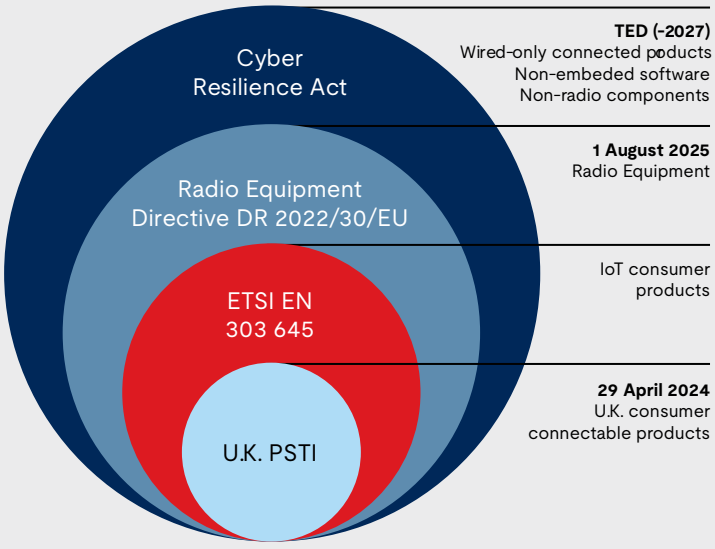
EU Radio Equipment Directive (RED) cybersecurity preparation (before hEN, June 30, 2024)

- **Gap analysis and certification against the remaining ETSI EN 303 645 provisions:**
  - Identify the gaps against the major part of the EU RED scope being covered by the ETSI EN 303 645 standards
  - Fill the identified gaps

EU RED cybersecurity final compliance (hEN release, June 30, 2024)

- **Fill the rest of the delta against the final Harmonized Standards hEN** (to be released, June 2024)

Cyber Resilience Act (date to be determined)



Key

Blue: regional regulations

Red: international standard, ETSI EN 303 645

UL Solutions

Safety. Science. Transformation.™

IMS24CS1550291