CRA Vs PSTI

Comparison Paper: UK PSTI Versus the EU CRA

29th April 2024

Cyber Cert Labs

cybercertlabs.com

How does the PSTI compare with the CRA?

On 29th April 2024 the UK Product Security and Telecommunications Act (PSTI) comes into force. Manufacturers of consumer products (or smart products) will need to ensure their products meet minimum security standards to comply with the act.

The regime comprises of two pieces of legislation:

- Part 1 of the Product Security and Telecommunications Infrastructure (PSTI) Act 2022; and
- The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

The act applies to manufacturers, importers and distributors of relevant connectable consumer products. The transition period for these businesses to prepare and comply was one year since April 2023.

The security requirements are set out in Schedule 1 of the regulation. These actions must be implemented to products that are in scope to address basic security and eliminate potential security vulnerabilities.

The security requirements relate to:

- banning universal default and easily guessable passwords
- publishing information on how to report security issues
- publishing information on minimum security update periods

There are additional duties for manufacturers, importers and distributors which include, but are not limited to, investigating potential compliance failures, duties to maintain records and duties to act in relation to compliance failures.

The law applies to any 'consumer smart device' that connects either to the internet, or to a home network (for example by Wi-Fi). This may include:

- smart speakers, smart TVs and streaming devices
- smart doorbells, baby monitors and security cameras
- cellular tablets, smartphones and games consoles
- wearable fitness trackers (including smart watches)
- smart domestic appliances (such as light bulbs, plugs, kettles, thermostats, ovens, fridges, cleaners and washing machines)

The regulation is based on a self-declaration and a statement of compliance digital or physical must accompany the product. There is a presumption of conformity for products that already align to the ETSI 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements. There is no third-party assessment required in terms of testing for compliance.

The Office for Product Safety and Standards (OPSS) will be responsible for enforcing the PSTI Act from 29 April 2024. OPSS is part of the Department for Business and Trade and already enforce the UK's existing product safety regulations.

The OPSS will use different mechanisms such as Compliance Notices, Stop Notices or Recall Notices to enforce the PSTI Act. Failure to comply with an enforcement notice is an offence liable on summary conviction to a fine. Financial penalties detailed below may be used also in relation to noncompliance:
Here we have mapped the main differences between the PSTI and the CRA:

Topic	PSTI	CRA
Reach	UK Only Manufacturers in scope are mainly outside the UK so impact is minimal in terms of UK businesses	EU – 27 member states Manufacturers in scope are widespread due to the wide scope of the CRA in EU member states and third countries
Enforcement	Office for Product Safety and Standards	Market Surveliance Authorities will be appointed.
Non-Compliance Penalties	The Act specifies the maximum penalty that may be imposed in relation to non-compliance. a) £10 million, or b) 4% of qualifying worldwide revenue for most recent accounting period The Act specifies the maximum penalty that may be imposed in relation to non-compliance that continues beyond the penalty deadline – the daily penalty element – as £20,000 per day. Under certain circumstances Stop Notices and Recall notices can be served.	Failure to comply with CRA essential requirements, vulnerability or incident reporting could incur penalties of: Administrative fines up to €15 Million or 2.5% of global turnover whichever is higher. Failure to comply with other obligations could incur penalties of: Administrative fines up to €10 Million or 2% of global turnover whichever is higher. Supplying misleading information to enforcement bodies or national CSIRT teams could incur penalties of: Administrative fines up to €5 Million or 1% of global turnover whichever is higher. Under certain circumstances EU authorities can require the recall or withdrawal of non-compliant products.

Products in Scope	Limited to Consumer connectable products i.e. IoT, smart products	Products with digital elements with a connection to a device or network including hardware, hardware with software or remote processing and standalone software, IoT, operational technology and other devices for consumers and business purposes. Websites, Cloud solutions and SaaS that do not support remote processing are not in scope. Open-source software that is developed outside of commercial activity is not in scope. Some products that already are covered by regulations such as medical devices, automotive are not covered by the CRA.
Assessment Type	Self-declaration through a statement of compliance	Depending on the criticality of the product category. It is estimated that 90% of products will fall into the non-critical default category which will require self-assessment, important products Class 1 and Class 2 will require third party assessment and use harmonised standards approach and critical product will require a formal conformity assessment under common criteria (EUCC)
Mapping to other standards	ETSI 303 645 Consumer IoT baseline of requirements and ISO/IEC 29147 vulnerability disclosure standard	Given the wide reach of the products in scope approximately 45 harmonised standards have been identified by ENISA as having overlap with some or most of the security requirements in the CRA.
Security Requirements Coverage	Limited to the top 3 principles in the Code of Practice for Consumer IoT Security. 1. No default passwords 2. Vulnerability disclosure 3. Software updates.	Comprehensive with security requirements based on 1. Security by design 2. Risk assessment 3. Vulnerability management 4. Vulnerability Disclosure 5. Security patching
Reporting Obligations	Manufacturers to supply one point of contact for reporting security issues. An	Manufacturers must report within 24 hours to their Nation CSIRT, followed by a more detailed report

	acknowledgement receipt and status updates until resolution must be sent to the reporter.	within 72 hours. A detailed vulnerability description and mitigation report is requirement within 14 days.
Documentation Requirements	The manufacturer, importer and distributor must ultimately ensure that the Statement of Compliance (SoC) accompanies the product and meets the necessary legal requirements in the PSTI Act 2022 and PSTI Regulations 2023.	To affix the CE mark you must follow the detailed documentation requirements in the Cyber Resilience Act in ANNEX II and ANNEX V in addition to producing the EU declaration of conformity in ANNEX IV.

Conclusion

In comparison with the Cyber Resilience Act (CRA) the PSTI is less robust and far reaching. This may be a deliberate phased approach for the UK to improve product security in stages. The requirements in the Cyber Resilience Act are comprehensive and in depth and will affect thousands of businesses in the EU and beyond. However, the PSTI will affect mostly non-UK IoT device manufacturers selling their products in the UK. This much smaller scope will have a benefit for supply chains and consumers but it is not the big bang that the CRA promises to be. We should expect more phases to come to cover more products including software and more comprehensive security requirements. This may be done in line with the CRA as it will not come into force until October 2024 with a transition period estimated at 3 years. There may be a possibility to agree on Mutual Recognition Agreement (MRA) with the UK if the PSTI and CRA closely align in the future.