PSTI Act 2022 FAQ

On April 2024, The UK government is implementing new products safety requirements for connected products under the Product Security and Telecommunications Infrastructure Act 2022, also known as PSTI.

From that date, organizations placing consumer connectable products on the UK markets must undergo PSTI verification, a mandatory requirement under new UK regulations.

Below we prepared a list of most often asked questions to guide you through the new legislation.

1

How can a distributor ensure compliance for products which he has for example today in stock and are not yet sold at the end of April 2024?

Distributors have a responsibility under the PSTI act to not supply non-compliant product. Therefore, they need to work with their suppliers/manufacturers to gain the necessary assurances that products they are currently selling are compliant. Ultimately the manufacturer should be able to produce a statement of compliance which the distributor can then provide to consumers along with the product.

Only one of the technical requirements of the PSTI directly relates to the product design – the requirements related to passwords. From our experience most products already satisfy this requirement as it is a long-established best-practice. The other requirements relate to the making available of information and can typically be resolved without requiring the products themselves to be modified.

2

Is the Statement of Compliance to be delivered or is it sufficient to have in the document accompanying the product a link to a website where the full Statement of Compliance can be downloaded?

There is no clear guidance on this, however our interpretation of the text of the regulation is that this must “accompany” the product. We do not think a link satisfies the requirement for the document to “accompany” the product.

3

Are you aware whether the Government has the intention to publish guidance for a better understanding of the legislation?

The government regularly updates the following webpage with information about the PSTI: https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

An explanatory memorandum to the PSTI was published on that page in January 2024 and it includes the following statement:

> Non-statutory Guidance to support industry compliance with the requirements in this instrument, and the broader product security regime, will be provided by the appointed enforcement authority for this regime – the Office for Product Safety and Standards. This guidance will be made available on the gov.uk website before the regime enters into force.

4 **Do Zigbee products such as relays fall into the scope of PSTI?**

Possibly. If it is a consumer product, and satisfies the following connectability conditions then it is likely to be in scope:

a. it is capable of connecting directly to two or more products at the same time by means of a communication protocol that does not form part of the Internet Protocol suite, and

b. it is capable of connecting directly to an internet-connectable product by means of such a communication protocol (whether or not at the same time as it connects to any other product).

5 **Our European suppliers advise that EN 303 645 is in the draft and the final version EN 18031-1 is not due to be finalized by CENELEC till June 2024 and is mandatory in August 2025. So will the UK standards change in the future?**

EN 303 645 is a published standard and is current. It has not been published as a British Standard, but it does form the technical basis for the UK Government's consumer IoT regulatory framework, currently the PSTI.

EN 303 645 is maintained by ETSI and there is no indication that it will not be maintained into the foreseeable future.

CENELEC is developing the EN EN 18031-1/2/3 standards to address the EU Radio Equipment Directive cybersecurity requirements and this will exist in parallel to EN 303 645 and the UK's PSTI. For products to be placed on the EU market, EN 18031-1/2/3 may become the more relevant standards (when finalised) but we cannot be certain until EN 18031-1/2/3 is published.

6 **Is the PSTI Regulation completely different to RED Article 3.3 (d), (e), (f), or does it complement it?**

It is completely separate. The PSTI only applies in the UK whereas the RED is part of EU law and relates to CE marking.

There are technical differences between the two legislations, for example the PSTI requirement to provide information on reporting vulnerabilities is not a requirement of the RED or the proposed harmonised standards EN 18031-1/2/3 (currently in draft).

7 **Do we know of any European/ US equivalent legislations that as an importer I could ask the supplier to comply with?**

The EU and US are in the process of introducing legislation covering product cybersecurity, however these are not relevant to PSTI compliance and importing product into the UK.

8 **Where, in the PSTI Act 2022, are the 3 specific security requirements defined, i.e. no default passwords, support policy, disclosure policy?**

These are not defined in the PSTI Act 2022, but in the accompanying PSTI Regulations 2023, accessible from here:

https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

9

Under the CPR door hardware does not require a physical paper DoP document to accompany the product, it was agreed this could be provided electronically by the manufacturer. Is this not the case with a Statement of Compliance for these products?

The PSTI is a separate piece of legislation from the CPR with its own requirements. Our understanding is that the PSTI is explicit in its requirement for products in scope to be accompanied by a statement of compliance.

10

If a system of non-compliant devices has been historically supplied, can replacement non-compliant devices be supplied, so that the original system can be maintained post-April 2024? That is, the replacement device has to be compatible with the existing device.

This is not an exception provided by the PSTI. The only consumer connectable products that are excepted from complying with the PSTI are those listed in Schedule 3 of the PSTI Regulations 2023, such as charge points for electric vehicles, medical devices, smart meter products and general purpose computers.

11

Regarding the usage of a password for a product, is it mandatory?

The PSTI does not mandate the use of passwords. The requirements for passwords only apply when passwords are used.

12

What about professional security systems that already have EN 50131, EN 50136, and RED Certificates? How do the PSTI requirements apply to such devices?

There is no requirement for manufacturers, importers and distributors of professional products that are not UK consumer connectable products or identical to UK consumer connectable products comply with the PSTI.

13

Can we adopt a 2-stage approach to compliance:

a. **Interim – until the manufacturer can implement ex-factory**
   Permanent – after the manufacturer has implemented ex-factory
b. **Temporary use of the QR code possible?**
   If the QR code is allowed, can it be positioned inside a product box?

Compliance must be achieved as of 29 April 2024. A temporary solution that meets the requirements would be acceptable, until a more permanent solution is implemented.

For example QR codes could be used to direct consumers to certain published information required by the PSTI, such as the information on how to report security issues. There are no requirements for QR codes themselves, if used.

14

Who is the enforcement body for PSTI compliance?

The Office for Product Safety and Standards (OPSS) is the Secretary of State’s chosen enforcing authority for Part 1 of the PSTI Act 2022, to support businesses to comply, and investigate, monitor, and take robust but proportionate enforcement action against those who do not comply.

15

What are Enforcement Notices and Sanctions?

Compliance notice – A notice requiring a person to comply with the relevant duty within a specified period.

Stop Notice – A notice requiring a person to stop carrying on a specific activity within a specified period if there are reasonable grounds to believe that non-compliance is/ will continue.

Recall notice – A notice requiring a person to make arrangements for the return of the products to themselves or another person, if there are reasonable grounds to believe that the is a compliance failure relating to products already supplied to the customer, i.e. if action taken is inadequate or if a Compliance/ Stop Notice/Forfeiture is not adequate to sufficiently manage risks.

Forfeiture – if the Secretary of State (SoS) has reasonable grounds to believe that there is a compliance failure relating to any forfeitable products that SoS may apply to the appropriate court for a forfeiture order and the products to be given specific person to be disposed of or destroyed.

Monetary penalties – if the Secretary of State (SoS) is satisfied on the balance of probabilities that there has been a compliance failure, they may issue a penalty of up to £10 million, or 4% of a company's worldwide revenue, along with daily fines of up to £20,000 where a breach continues.

Offenses – Non-compliance with enforcement notice
Obstructing an enforcement officer
Purporting to act as an enforcement officer.

16

What products are in scope of the PSTI?

Consumer connectable products, including but not limited to:

- Smartphones
- Connected cameras, TVs and speakers
- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Internet of Things stations and hubs to which multiple devices connect
- Wearable connected fitness trackers
- Outdoor leisure products, such as handheld connected GPS devices that are not wearables
- Connected home automation and alarm systems
- Connected appliances, such as washing machines and fridges
- Smart home assistants

Paragraphs 4 and 5 of the PSTI Act 2022 (Part 1) provide a detailed logic for determining if a consumer connectable product is in scope.

https://www.legislation.gov.uk/ukpga/2022/46/part/1/enacted

Find out more
Call: **+44 (0)345 0765 606**
Email: **product.certification@bsigroup.com**
or visit: **bsigroup.com/iot**