

Europe *UK*

Internet of Things: proposals for cyber security regulation

The UK government is considering moving towards regulating security standards for consumer Internet of Things (“IoT”) devices. The Department for Digital, Culture, Media and Sport pushed ahead with a consultation process in May 2019 around proposals for regulation, though the UK government had only recently published a voluntary code of practice – the Code of Practice for Consumer IoT Security – in October 2018.

The voluntary code published in October promoted 13 principles for IoT security

- no use of default passwords
- provision of a public point of contact for anyone concerned about security vulnerability
- keeping software updated and telling consumers the minimum length of time that their device will be supported
- secure storage of credentials and personal information
- secure management of information flow
- minimising potential points of attack, including turning off unused functions
- maintaining software integrity and preventing unauthorised software changes
- compliance with GDPR
- resilience to power loss and network unavailability
- usage monitoring for security anomalies
- consumers able to delete personal data
- updates and maintenance should be easy for consumers involving minimal steps and
- data in-putted should undergo validation.

It was followed in the EU with the same 13 principles being reworked into an EU-recognised technical standard ETSI 103 645 “Cyber Security for Consumer Internet of Things”, published in March 2019.

Security by design is fundamental

The prompt for action by UK regulators is concern that as more devices in the home connect to the internet, consumers are entrusting their personal data to an increasing number of online devices and services. Products and appliances that have traditionally been offline are now becoming connected and exposed to cyber threats. Margot James has stated that “security by design is fundamental if we are to progress with the internet of things”.

So, after only seven months of the code of practice being live in the UK (the consultation period was relatively short, opening on 1 May and closed on 5 June) the UK Government is looking at moving from voluntary adoption of best practice to mandating how companies should design their IOT consumer devices and products.

The UK Government wants to introduce three mandatory requirements for connected devices based on three of the principles from the Code of practice and ETSI standard

- No default passwords: All IoT device passwords shall be unique and shall not be resettable to any universal factory default value
- Providing a public point of contact: The manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues
- Telling consumers how long the product would be supported: Manufacturers will explicitly state the minimum length of time for which the product will receive security updates.

The consultation process has also included proposals around how information about the IOT security measures proposed should be communicated to consumers to demonstrate that the product complied with IOT security regulations. A new mandatory or voluntary labelling scheme is being proposed.

Consultation on the scope of implementing regulations

The UK Government is considering three options for implementation

- Option A (preferred option): Mandate retailers to only sell consumer IoT products that carry the proposed IoT security label, with manufacturers to self-assess and implement a security label on their consumer IoT products
- Option B: Mandate retailers to only sell consumer IoT products that adhere to the “top three guidelines” of the Code of Practice for IoT Security, with manufacturers to self-assess that their consumer IoT products adhere to these top three guidelines and
- Option C: Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers expected to self-assess and to ensure that the label is on the appropriate product packaging.

Following the consultation and after the introduction of the voluntary security labelling scheme, the UK Government said it would make a decision as to which of the above options should be taken forward into legislation.²⁴ Now with a new Minister and Prime Minister in office it will be interesting to see if policy changes or the planned regulation is delivered.



Lucy Ward
Legal Consultant, London
T +44 20 7296 2898
lucy.ward@hoganlovells.com

²⁴ See also <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>