

United Kingdom Establishes IoT Security Principles

Article By:

Doneld G. Shelkey

Katherine B. O'Keefe

The UK government recently released a policy paper outlining proposed requirements for makers of Internet of Things (IoT) devices to take certain actions to better protect IoT devices from growing cybersecurity threats. [Secure by Design: Improving the cyber security of consumer Internet of Things Report](#) was released by the UK's Department for Digital, Culture, Media & Sport and contains a draft Code of Practice for manufacturers of consumer IoT devices and services.

Some of the actions suggested by the draft Code of Practice include the following:

- **No default passwords.** All IoT device passwords must be unique and follow best practices on passwords and other authentication methods.
- **All companies providing IoT devices and services must have a public point of contact for reporting issues.** In addition, companies should act promptly on remedying any reported issues and are encouraged to share information with relevant industry bodies.
- **Companies must keep all IoT software updated.** Updates should not impact the functionality of the IoT device and companies must publish an end-of-life policy stating the minimum length of time that a device will receive software updates. Any update should be accompanied with the reason for the update.
- **Personal data should be processed in accordance with applicable data protection laws.** IoT device manufacturers need to communicate with customers about how their personal data is being used, by whom, and for what purposes. Any consent to processing personal data must be obtained lawfully. Manufacturers should provide information on how to securely set up and dispose of IoT devices.
- **Customers should be able to delete their personal data easily.** IoT devices should be configured so that personal information can be easily deleted whenever the customer wishes to do so.

The public may comment on the draft Code of Practice through April 25, 2018. The report makes clear that its recommendations are in draft form and are part of a continuing effort to address cybersecurity concerns in connection with new technologies, which may result in new guidelines or, if necessary, new laws or regulations.

Copyright © 2025 by Morgan, Lewis & Bockius LLP. All Rights Reserved.

National Law Review, Volume VIII, Number 81

Source URL: <https://natlawreview.com/article/united-kingdom-establishes-iot-security-principles>