compliance & risks

Welcome

The Convergence of Product Safety & Cybersecurity Laws and Regulations

Presented by: Sarah-Jane Dobson, Kennedys

At Compliance & Risks

We help our clients monitor and manage regulations, standards, requirements and evidence to better mitigate risk.

Peace of mind

Brand protection

Increased market access

Future proofing of the business by aligning with global trends

End-to-End Regulatory Solutions

Market Access

- Customized research
- Consider new products & countries
- Compare obligations in multiple jurisdictions
- Understand regulations at a high level or deep analysis

C2P Platform

- Regulations, standards, requirements & evidence
- Proposed & enacted regulations
- Global daily monitoring and alerts
- Efficient workflow tools
- Knowledge Management
- SME support

Managed Services

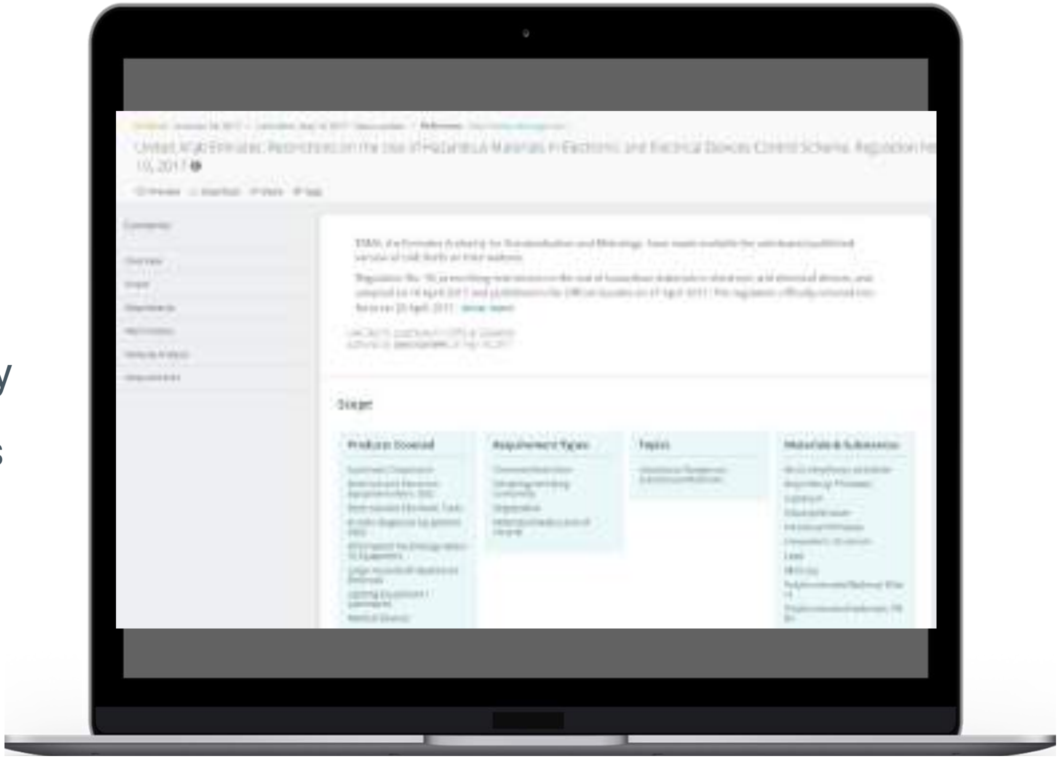
- Fulfil specific compliance functions
- Full suite of compliance skills
- 23 languages
- On-site and/or off-site delivery

Benefits

Sooner: advanced warning of trends and proposed regulations

Faster: understanding of regulations that matter with structured content, English summaries and the support of our regulatory compliance experts and knowledge partners

Better: all relevant content in one platform, along with the team’s analysis and actions



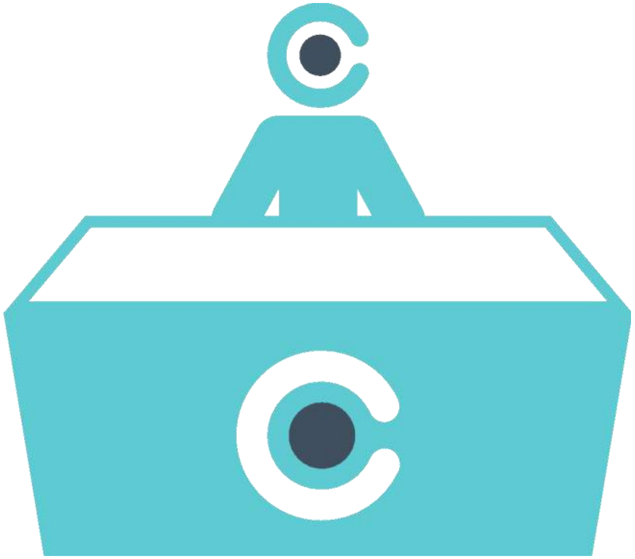
Answering Your Questions

Ask Our Experts

- Premier access to our global regulatory compliance team
- Your questions answered about regulations

Knowledge Partners

- Our global network shared with you
- Legal, business, supply chain and environmental specialists
- Providing ‘on the ground’ expert knowledge on hot topics
- Breaking news and analysis via your alerts



The Convergence of Product Safety & Cybersecurity Laws and Regulations

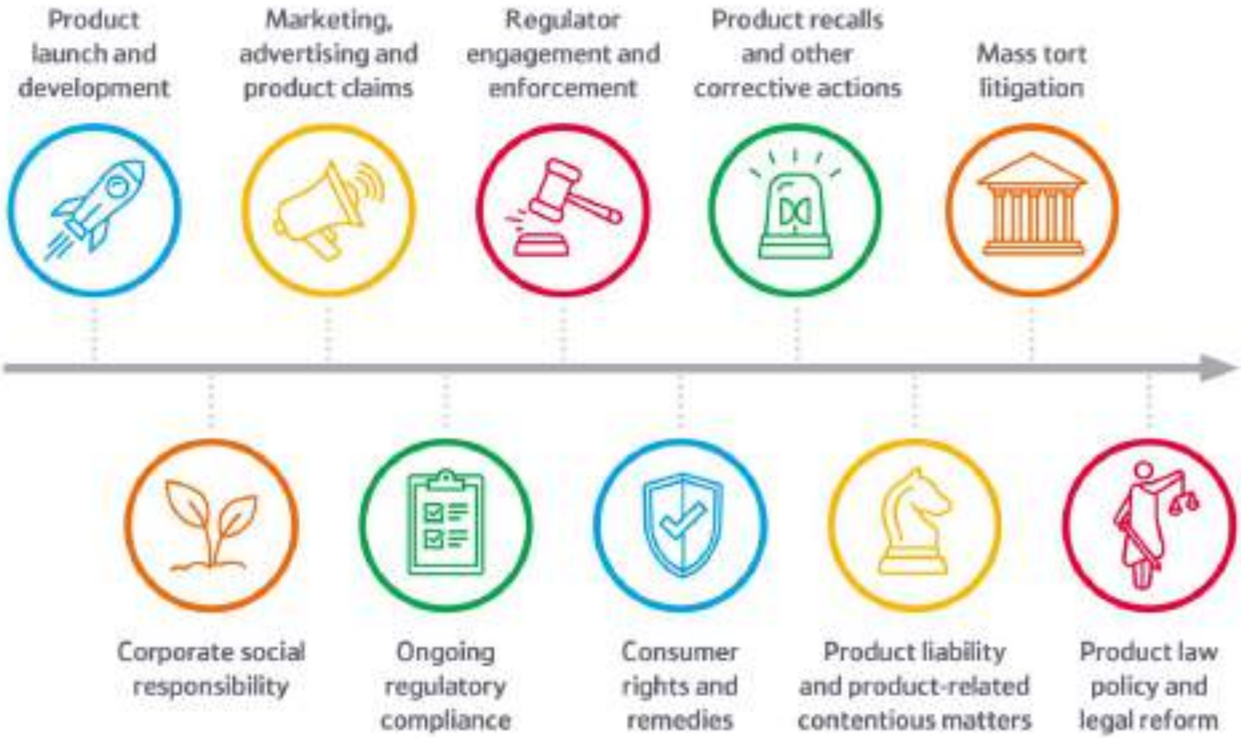
The convergence of product safety and cybersecurity laws and regulations

Sarah-Jane Dobson

9th November 2021

Kennedys

Kennedys Product Safety and Liability Team



Product launch and development

Marketing, advertising and product claims

Regulator engagement and enforcement

Product recalls and other corrective actions

Mass tort litigation

Corporate social responsibility

Ongoing regulatory compliance

Consumer rights and remedies

Product liability and product-related contentious matters

Product law policy and legal reform

Agenda

Common cyber-attacks on Products	3
Legislative history of key product safety and cybersecurity regimes	8
How is cybersecurity regulated in the EU and UK?	10
Which products will be most impacted?	20
Likely future developments	27
Practical tips and takeaways	30

Cyber-attacks in context

Cyber-attack vulnerability on Jeep cars

- In 2015, Fiat Chrysler recalled 1.4 million vehicles after finding that the Jeep Cherokee could be hacked
- Researchers found they could be hacked via the entertainment system
- The Wi-Fi was used to hack the vehicle as passwords are generated automatically based on the time the car and multimedia system are turned on
- Various systems could be controlled/accessed such as the music player, and the GPS locator
- One researcher, Charlie Miller, said following the recall:

  "I wonder what is cheaper, designing secure cars or doing recalls?"

Cyber-attacks in context

Cyber-attack vulnerability on Jeep cars

Source: https://www.youtube.com/watch?v=RZVYTJarPFs

QUIZ

Have you ever experienced a cyber-attack first-hand?

- Yes
- No
- I’m not sure

Common cyber-attacks using Products

DDOS and Botnets

QUIZ

What is a ‘botnet’?

- a) A net that catches window-cleaning robots
- b) A collection of websites for buying robots
- c) A network of internet-connected devices infected with malware
- d) A network of fake social media accounts

ANSWER

What is a ‘botnet’?

- a) A net that catches window-cleaning robots
- b) A collection of websites for buying robots
- c) A network of internet-connected devices infected with malware
- d) A network of fake social media accounts

Cyber-attacks on Products

DDOS and Botnets

- Distributed Denial of Service (DDOS)
- Target server overwhelmed and forced offline
- IoT devices used to make botnet
- IoT devices used without users' consent or knowledge

Cyber-attacks on Products

DDOS and Botnets

CASE STUDY 1 – Mirai Botnet Attack

- Occurred in 2016
- 61 username/password combinations used to hack devices
- Launched initially against cybersecurity journalist
- Code leaked and used widely
- Lesson = avoid simple and universal default passwords

Legislative history of key product safety and cybersecurity regimes

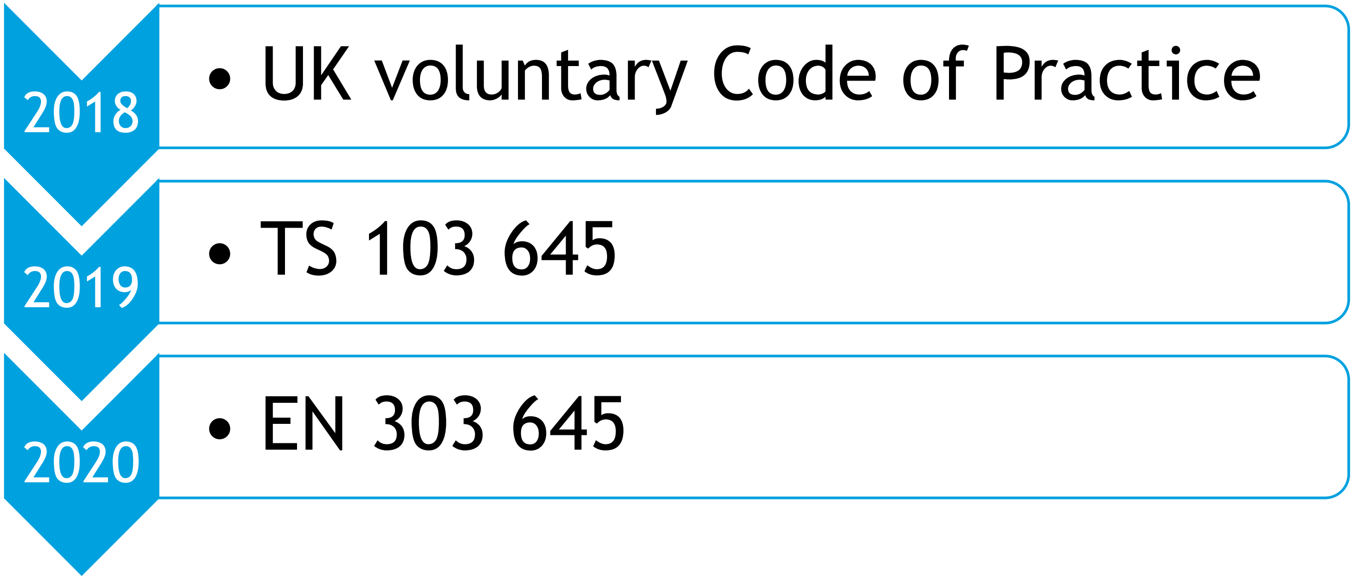
Kennedys

Legislative history

EU and UK

2008 Commission Staff Working Document

EU Cyber Security Strategy (EUCSS)



2018
- UK voluntary Code of Practice

2019
- TS 103 645

2020
- EN 303 645

How is cybersecurity regulated?

European Union

Kennedys

European Union Regulations

Proposed Regulations

Cyber Resilience Act announced at the second State of the Union address in September 2021

Revised General Product Safety Directive (GPSD) proposals

Proposed delegated regulation under Radio Equipment Directive (RED) obligating manufacturers to improve cybersecurity of certain wireless devices

European Union Regulations

Delegated Regulation under RED

- Proposal to place obligations on manufacturers to improve cybersecurity of certain wireless devices that utilise radio technology
- Applies to EU and non-EU manufacturers who place products on the European market
- Proposed requirements include:
  - Preventing harm to networks
  - Guarantee privacy of personal data
  - Reduce risk of fraud if device used for electronic payments
- Aims of the regulation are general, not technical
- The European Commission will request a standard to be developed with technical solutions

European Union Regulations

Revised GPSD proposals

- Revision to 20-year-old legislation

- Proposed amends:
  - New definition of product to cover interconnectivity
  - Free software updates as a right of remedy
  - Inclusion of international and European standards along with expert opinions to assess the safety of products

European Union Regulations

Cybersecurity Act

- Came into force on 27 June 2019
- Has applied across the EU since 28 June 2021
- Its purpose:
  1. To grant ENISA its mandate and role; and
  2. To establish a cybersecurity certification scheme

European Union Regulations

Cybersecurity Act - cybersecurity certification framework

- ICT products must comply with specified requirements

- Certification is voluntary but creates a presumption of compliance

- Key objectives of certification are to:
  - Protect data from unauthorised storage, processing, access, or disclosure
  - Identify and document known dependencies and vulnerabilities
  - Verify that the product does not contain known vulnerabilities
  - Ensure products are secure by default and design

- Categories of assurance levels are:
  - Basic
  - Substantial
  - High

European Union Regulations

Regulatory Standards

TS 103 645

- Published February 2019
- First globally applicable industry standard
- Based off UK CoP
- Includes data protection provisions

European Union Regulations

Regulatory Standards

EN 303 645

- Published June 2020
- Baseline for product cybersecurity
- Designed to prevent large-scale attacks

How is cybersecurity regulated?

United Kingdom

Kennedys

UK Regulations

Voluntary Code of Practice

- Published in March 2018
- Sets out 13 guidelines to protect consumers
- Focused on proactive secure-by-design approach to cyber security

UK Regulations

Potential future regulation

- UK Government have responded to call for views on proposals for UK domestic legislation
- National Cyber Security Strategy
- Powers for enforcement authority to investigate non-compliance

Which products will be most impacted?

IoT medical/fitness devices and Children's toys

Kennedys

Most Impacted Products

IoT medical/fitness devices

- Grey zone between fitness and medical devices
- Fitness devices are less strictly regulated and left to self-regulation
- Storage of sensitive health data
- Design flaws and mass manufacturing means devices are easy to hack

QUIZ

What is the Internet of Children’s Things (IoCT) market expected to be worth in 2023?

- a) $800 million
- b) $2 billion
- c) $10 billion
- d) $18 billion

ANSWER

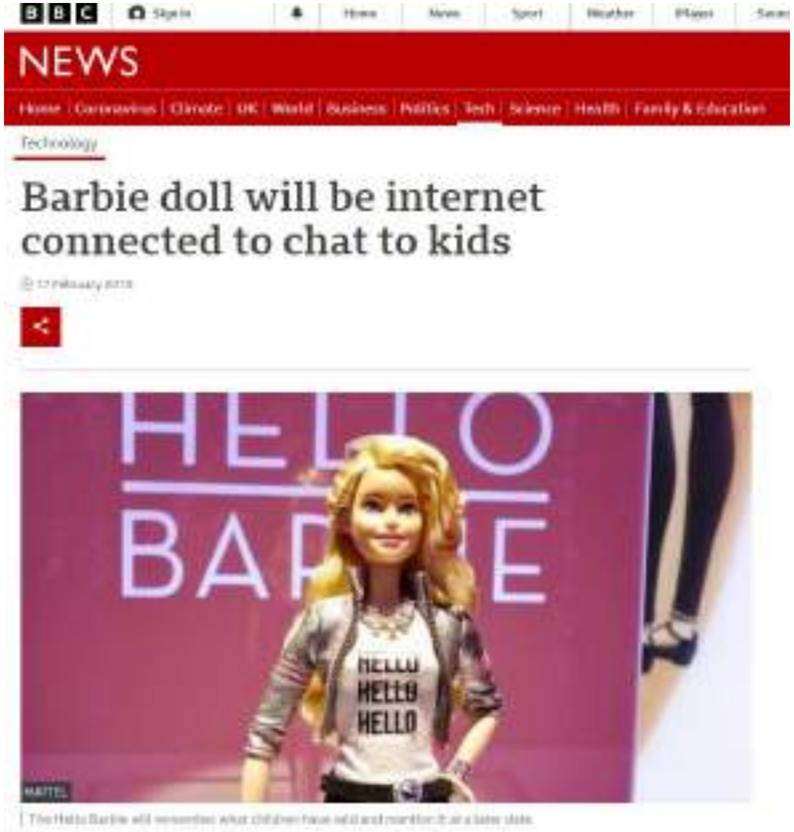
What is the Internet of Children's Things (IoCT) market expected to be worth in 2023?

- a) $800 million
- b) $2 billion
- c) $10 billion
- **d) $18 billion**

Most Impacted Products

IoT children’s toys

- Basic design flaws leave children’s products vulnerable to being hacked
- Particularly concerning given users are minors and are not always supervised by parents
- Wi-Fi and Bluetooth features are primary vehicles for hacking
- Hello Barbie doll raised concerns in 2015


BBC
Sign in
Home
News
Sport
Weather
iPlayer
NEWS
Home | Coronavirus | Climate | UK | World | Business | Politics | Tech | Science | Health | Family & Education
Technology
HELLO
BARBIE
HELLO
HELLO
HELLO
MATTEL

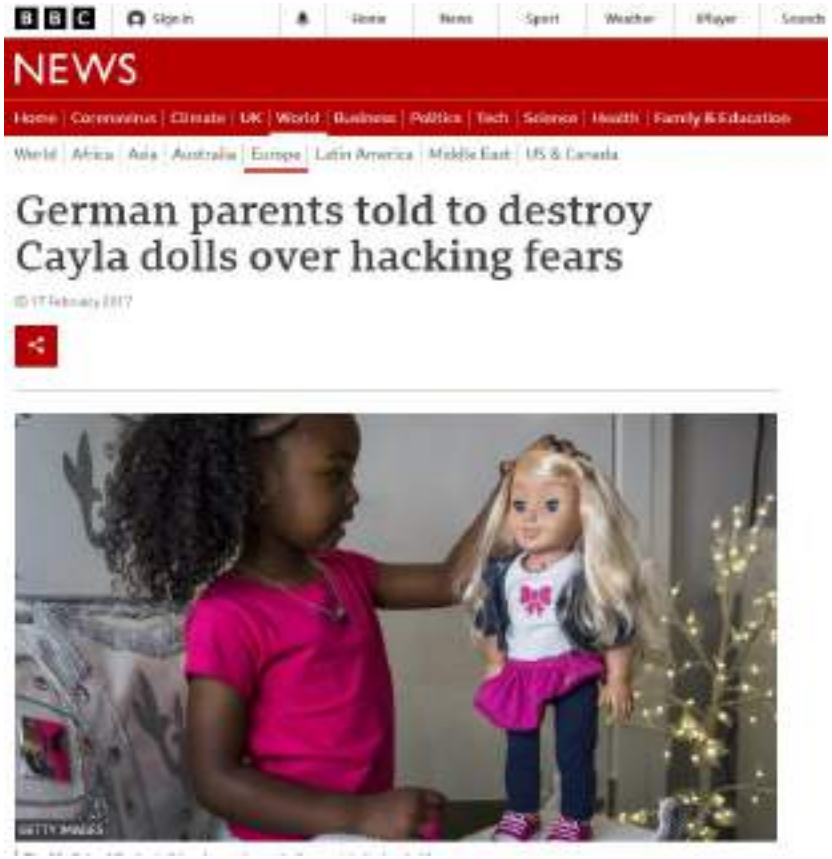
Barbie doll will be internet connected to chat to kids

17 February 2015

The Hello Barbie will remember what children have said and mention it at a later date

Most Impacted Products

IoT children’s toys


BBC
Sign in
Home
News
Sport
Weather
iPlayer
Search
NEWS
Home | Coronavirus | Climate | UK | World | Business | Politics | Tech | Science | Health | Family & Education
World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

German parents told to destroy Cayla dolls over hacking fears

17 February 2017

GETTY IMAGES

CASE STUDY 1 - Cayla dolls

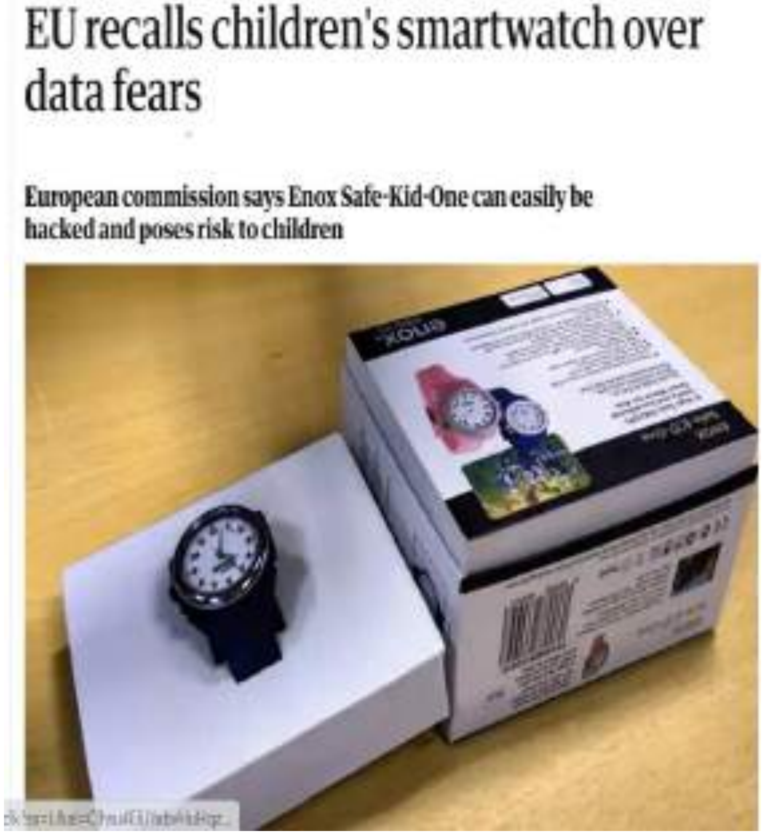
- German watchdog ordered for the destruction of the doll in 2017
- Unsecure Bluetooth device could be hacked
- Unauthorised users could eavesdrop on child user’s conversations

Most Impacted Products

IoT children's toys

<u>**CASE STUDY 2 – Enox Safe-Kid-One**</u>

- European Commission recalled the watch in 2019
- Child user's location could be tracked and data stolen
- Highlights the growing concern in the children's smartwatch industry



EU recalls children's smartwatch over data fears

European commission says Enox Safe-Kid-One can easily be hacked and poses risk to children

Likely future developments

The UK and EU

Kennedys

Likely future developments

Legislative

UK

- UK Government stated they will legislate on this area
- Legislation likely based off Code of Practice
- Potential for specific medical/fitness device and IoCT provisions

EU

- Unclear when revised GPSD will be passed
- More certification schemes under Cybersecurity Act
- Proposed RED Delegated Regulation expected to come into force in mid-2024 (30-month transition)

Likely future developments

Practical

- Increased product recalls
- Increased product liability claims
- Increased costs to ensure secure by design manufacturing
- Setting up of specific manufacturer in-house teams focused on researching and developing cyber security of products as regulations develop
- Collaboration/increasingly blurred lines between regulator's enforcement areas
- Increased regulator powers

Practical tips and takeaways

Kennedys

QUIZ

Is your company planning to improve the current cyber security of its products?

- Yes
- No
- I’m not sure

Practical tips and takeaways

- Set out full capabilities of the IoT device
- Proactive instead of reactive approach
- EU certification
- Avoid simple universal default passwords
- Ensure the regulations of the various countries where the product will be supplied are understood – Amazon Ring Doorbell

Q&A

Sarah-Jane Dobson

Partner

t +44 20 7667 9677

m +44 7436 039 677

e sarah-jane.dobson@kennedyslaw.com