STEVENS&BOLTON

EUROPEAN CYBER RESILIENCE ACT

The European Cyber Resilience Act (CRA) is an EU proposal to regulate cybersecurity requirements for products with digital elements. As at November 2023, a final version of the proposed regulation is awaited.

WHAT DOES THE CRA AIM TO DO?

It is recognised that many products, including everyday consumer products, are increasingly "connected" to each other and a variety of systems, increasing the risks and damage caused by cyber-attacks, especially as some products currently can be a relatively easy entry point for malicious actors. The explanatory memorandum to the CRA had estimated that the annual cost of cybercrime for 2021 was in the region of EUR 5.5 trillion by 2021, noting that cyber attacks can have a severe impact on economic and social activities and can even be life threatening.

The CRA therefore aims to ensure:

- Products with digital elements (PDEs) placed on the EU market have fewer security vulnerabilities, and
- Manufacturers consider security throughout a product's life cycle by design.

WHAT IS A PDE?

The CRA provides that a PDE means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the EU market separately. Examples include connected home cameras, smart fridges and smart televisions.

Certain products are excluded where already subject to specific sector regulations. For example, medical and in-vitro medical-diagnostic devices, motor vehicles, PDEs developed for national security or military purposes and products specifically designed to process classified information.

WHICH BUSINESSES DOES THE CRA IMPACT?

The CRA will affect all levels of the supply chain – manufacturers, importers and distributors of PDEs. where a product is placed on the EU market. It therefore has the potential to affect those UK businesses that supply or manufacture for the EU.

WHAT ARE THE KEY REQUIREMENTS FOR MANUFACTURERS?

1. **Cyber security risk assessments**. The manufacturer must carry out Cyber security risk assessments and included these within the technical documentation which accompanies the PDE when it's placed on the EU market.

2. **Due diligence**. The manufacturer must carry out due diligence to ensure the PDEs fulfil essential cybersecurity requirements (e.g. protect against unauthorised data access).

3. **Conformity assessments**. The manufacturer must carry out conformity assessments of the essential requirements and any vulnerability handling requirements. If a PDE conforms, it needs to be supplied with an EU declaration of conformity (or link to the declaration). The manufacturer must also take immediate corrective measures (e.g. withdrawal from the market or recalling the product) if it is subsequently discovered the product is not conformant. This requirement lasts for the lifetime of the product, or five years from being placed on the market, whichever is shorter.

4. **Managing vulnerabilities**. The manufacturer must identify and document vulnerabilities, apply regular testing, provide security updates and provide a contract address for reporting vulnerabilities. This requirement lasts for the lifetime of the product, or five years from being placed on the market (whichever is shorter).

5. **Incident reporting**. The manufacturer must report an exploited vulnerability to the EU Agency for Cybersecurity (ENISA) without undue delay and in any event within 24 hours.

6. **Technical documentation**. The manufacturer must create and maintain technical documentation, with all relevant data of the means used by the manufacturer to ensure the PDE and processes in place to comply with the essential requirements.

7. **Authorised representatives**. The manufacturer must appoint authorised representatives to perform specific tasks required by the CRA.

WHAT ARE THE KEY OBLIGATIONS FOR IMPORTERS AND DISTRIBUTORS?

1. Carry out due diligence before making a PDE available on the EU market - ensure that: the relevant conformity assessment has been carried out by the manufacturer; CE marking has been affixed and the PDE is accompanied by the relevant information, documentation and instructions.

2. Inform the manufacturer of a vulnerability without undue delay if they have reason to believe that a PDE presents a significant cybersecurity risk.

WHO OVERSEES COMPLIANCE?

State Level

EU member state market surveillance authorities are responsible for monitoring compliance at member state level. Tasks include evaluation of the CRA at a national level, evaluation of PDEs with a significant cybersecurity risk, issuance of guidance to operators, imposition of corrective and restrictive measures and issuing penalties.

EU level

- The Administrative Cooperation Groups have a supervisory role to ensure the uniform application of the CRA.
- The European Commission also has a central role and exclusive powers in the supervision and enforcement of the CRA and responsibility to ensure that member states adopt decisions in line with EU law.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Fines

- Fines range from €5,000,000 – €15,000,000 or 1-2.5% of worldwide turnover in the preceding financial year, whichever is higher. For manufacturers, breaches of essential requirements, conformity assessment and reporting obligations may result in fines of up to €15,000,000 or 2.5% of annual global turnover, whichever is higher.
- For importers and distributors, there could be fines of up to €10,000,000 or 2% of the annual global turnover, whichever is higher.
- Manufacturers, importers or distributors which provide incorrect or misleading information face fines of up to €5,000,000 or 1% of annual turnover.

Corrective or restrictive measures.

In addition to fines, relevant authorities can require the recall or withdrawal of products from the EU market.

HOW DOES THE CRA IMPACT THE UK?

Although it is a piece of EU legislation, the CRA will affect many UK businesses. As noted above, the CRA would apply to a UK-based business to the extent it places products with digital elements on the EU market or manufactures for that market. In addition, the CRA covers remote data processing solutions so could potentially cover processing outside of the EU, including the UK.

More generally, it may be that the CRA becomes the global standard for product security, similar to the General Data Protection Regulation, in which case companies that operate internationally may decide to comply with the CRA across their operations.

THE UK CYBERSECURITY REGULATION

In addition, there is incoming cybersecurity legislation in the UK: the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 has been published which applies to "connectable products". Businesses with both an EU and UK market will need to understand and comply with both sets of incoming regulations.

KEY CONTACTS

For further information about any of the issues raised in this guide, please contact:

Beverley Flynn
Head of Commercial & Technology
T: +44 (0)1483 734264
M: +44 (0)7769 708486
E: beverley.flynn@stevens-bolton.com

Guy Cartwright
Managing Associate
T: +44 (0)1483 734235
M: +44 (0)7581 055083
E: guy.cartwright@stevens-bolton.com

STEVENS&BOLTON

Wey House, Farnham Road
Guildford, Surrey, GU1 4YD
Tel: +44 (0)1483 302264
Fax: +44 (0)1483 302254
DX 2423 Guildford 1
www.stevens-bolton.com

DEPARTMENTAL\60327117v1