THE MANUFACTURING TECHNOLOGIES ASSOCIATION

Manufacturing Technologies Association

Technical - Legislation Updates

Contents

UK Carbon-Border-Adjustment-Mechanism – UPDATE

What is the UK Carbon-Border-Adjustment-Mechanism (CBAM)?

The UK Carbon-Border-Adjustment-Mechanism (CBAM) is a policy set to be introduced by January 2027.

It aims to place a carbon price on the emissions intensity of imported goods to ensure they face a comparable carbon price to those produced within the UK. This mechanism is intended to mitigate carbon leakage by applying a carbon price to imported goods, ensuring they are subject to a comparable carbon price as UK-produced goods.

What products does the UK Carbon-Border-Adjustment-Mechanism apply to?

The CBAM will apply to the emissions embodied in imports of specified goods from seven sectors: aluminium, cement, ceramics, fertilisers, glass, hydrogen, and iron & steel.

When does CBAM apply and Who is responsible?

Time in which CBAM liability arises will be either:

- where a good is subject to customs control, the date on which the good is released into free circulation, or
- where there are no customs controls, the date on which the CBAM good first enters the UK.

No need to register or account for CBAM if the total value of their CBAM goods passing a tax point falls below a minimum registration threshold of £10,000 over a rolling 12-month period.

The government is suggesting that individuals who meet a certain threshold will need to register for CBAM, either when they expect to meet the threshold or when they actually do, whichever comes first.

The liable person for the CBAM charge will be either?

- where there are customs controls, the person responsible for the goods when they are released into free circulation. This means the liable person could be the importer of the CBAM goods, but this is not always the case (for example where there is a change of ownership while the goods are under customs control),
- or where there are no customs controls, the person on whose behalf the goods are moved to the UK.

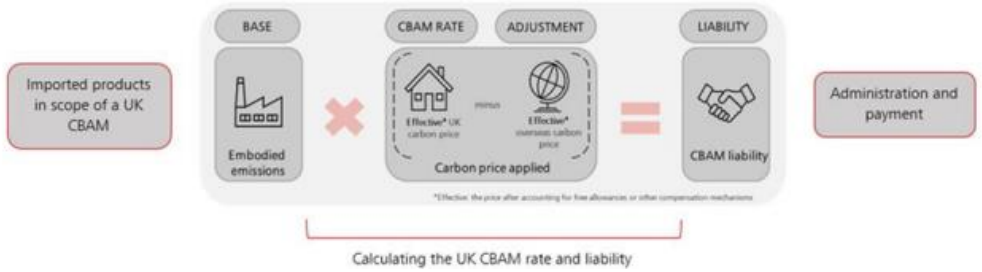
How is the liability determined?

The CBAM liability will be calculated by multiplying the total emissions emitted per type of good by the relevant UK CBAM rate, minus the carbon price payable overseas.

In terms of calculating the emissions, the government proposes that the liable person will either:

- provide information about the emissions associated with their CBAM goods, verified by an independent verification body, or
- apply default emissions values which the government will publish – these will be based on a global weighted average of UK imports for the relevant sector

The government plans to establish the rate for CBAM goods, with seven rates proposed, each corresponding to a specific sector. This means that all taxable iron & steel goods will have one rate, while all taxable aluminium goods will have another, and so forth.



Calculating the UK CBAM rate and liability

When will the Act take effect & what are the penalties for non-compliance?

The CBAM will take effect from January 2027.

There are currently no specific details on penalties for non-compliance, but it is expected that there will be administrative burdens and potential financial penalties for failing to meet the reporting and payment obligations.

How will it impact UK companies and what should they do now?

- The introduction of the UK CBAM will level the playing field for domestic producers by imposing a carbon price on imported goods from specified sectors,
- This will reduce competitive disadvantages.
- UK companies will face increased costs and administrative burdens as they need to report emissions and comply with new regulations
- Leading to higher prices for consumers and supply chain adjustments.

To prepare, UK companies should familiarize themselves with the CBAM requirements, engage in consultations, assess their supply chains for emissions data, and set up compliance systems. They should also plan for potential cost increases and enhance their sustainability initiatives to reduce their carbon footprint and align with broader corporate and national climate goals.

Product Security & Telecommunications Infrastructure (PSTI) Act - Update

What is the PSTI Act

The Product Security and Telecommunications Infrastructure Act 2022 enhances security for internet-connectable products and those capable of connecting to them. It also includes provisions for electronic communications infrastructure.

What Product does the Act apply to?

The Act applies to "relevant connectable products," which include any internet-connectable consumer products or products that can connect to other internet-connectable devices.

Who has obligations under the Act, and what are the key obligations?

Obligations under the Act fall primarily on manufacturers, importers, and distributors of relevant connectable products:

Manufacturers: Must ensure their products comply with specified security requirements and provide a statement of compliance with each product. They are also responsible for rectifying any security failures.

Importers: Must ensure that the products they import meet the security requirements and retain documentation of compliance. They must not make non-compliant products available in the UK.

Distributors: Must ensure the products they distribute are compliant with security requirements. They must take reasonable steps to rectify any compliance failures and notify relevant parties of such failures.

What are the essential requirements?

Essential security requirements include:

- Provision of a statement of compliance by manufacturers.
- Adherence to specified security measures to protect the product and its users.
- Ensuring compliance and rectification of any failures related to security requirements

When will the Act take effect, and what are the penalties for non-compliance?

The **UPDATED** Act took effect on April 29, 2024. Penalties for non-compliance can include fines, enforcement actions, and possible forfeiture of non-compliant products.

How will it impact UK companies, and what should they do now?

UK companies involved in the manufacturing, importing, or distributing of connectable consumer products will need to ensure compliance with the new security standards.

This includes updating product security measures, maintaining appropriate documentation, and being prepared to address any compliance issues promptly.

Companies should start auditing their products and processes now to align with the Act's requirements before it comes into force.

Report any security breaches and cooperate with regulatory authorities (OPSS) and provide security guidance to customers (i.e. how to remain secure and minimise any risks).

EU Critical Raw Materials Act – MAGNET REVISION

The CRMA introduces several regulatory requirements for natural and legal persons placing goods on the market. These can be found in Articles 28 to 34, and include the following:

Recyclability of permanent magnets

- New labelling requirement indicating the incorporation for permanent magnets for a range of goods in advanced manufacturing sectors and for white goods, which must also include data carriers confirming details of responsible individuals and magnetic composition.
- Making information on recycled content of permanent magnets accessible and providing information to customers when selling goods.

Environmental footprint declarations

- Making available and publishing environmental footprint declarations for each individual critical raw material type placed on the market. *This will not apply to critical raw materials included in intermediate or final products*.
    - This will require a list of details, including e.g., information about the country and region where the critical raw material was extracted, processed, refined and recycled.

Free movement

- Permitting persons displaying products with permanent magnets or critical raw materials for demonstrative purposes e.g., at trade fairs or exhibitions, providing the product is suitably labelled or signposted, noting it cannot be made available on the market until it complies with the Regulation.

Conformity and market surveillance

- Ensuring persons placing products on the market covered by recyclability of magnets and footprint declaration requirements carry out applicable conformity assessment procedures, drawing of technical documentation and affixing CE markings.

Article 28 – Recyclability of permanent magnets

- Natural or legal persons placing a specified list of goods on the market will be required to attach clear labelling indicating whether the products incorporate one or more permanent magnets, and whether those permanent magnets belong to the following types: neodymium-iron-boron; samarium-cobalt; aluminium-nickel-cobalt; ferrite.

- They will also need to include a data carrier which is linked to a unique product identifier which confirms the contact details of responsible individuals, information on magnetic composition, and details informing access/removal of incorporated magnets. This must be

consistent with Article 15(1) of the Waste Electrical and Electronic Equipment Directive 2012/19/EU. Where a digital product passport is required in other EU legislation, the relevant information must also be included in the product passport.

- In doing so, they will need to ensure that they meet relevant requirements in providing the information for a specified period, including to repairers, recyclers, market surveillance authorities and customs authorities.

- This concerns the following list of goods:
    - magnetic resonance imaging devices,
    - wind energy generators,
    - industrial robots,
    - motor vehicles,
    - light means of transport,
    - cooling generators,
    - heat pumps,
    - electric motors, including where electric motors are integrated in other products,
    - automatic washing machines,
    - tumble driers,
    - microwaves,
    - vacuum cleaners
    - dishwashers

Article 29 – Recycled content of permanent magnets

- Natural or legal persons placing products on the market which incorporate one of more permanent magnets of the neodymium-iron-boron; samarium-cobalt; or the aluminium-nickel-cobalt type (ferrite is not captured by this requirement), and where the total weight of all permanent magnets exceeds 0,2 kg, shall make publicly available the share of recovered post-consumer magnetic waste present in the permanent magnets. This concerns the following critical raw materials: neodymium, dysprosium, praseodymium, terbium, boron, samarium, nickel and cobalt.

- The European Commission will adopt a delegated act to supplement the Regulation in no less than two years from entry into force of the Regulation to establish rules for the calculation and verification of the share of the abovementioned CRMs. These rules will also specify the applicable conformity assessment procedures and consider any necessary adaptation for relevant products, with specific reference to modules set out in Annex II to Decision No 768/2008/EC and considering product safety and risk as well as the need for third party conformity assessment.

- The placing on the market obligations will come into force either three years from the entry into force of the Regulation, or two years from the entry into force of the abovementioned delegated act, whichever is later.

- Once the calculation and verification rules are established via the delegated act, and no later than 31 December 2031, the Commission will adopt delegated acts to supplement the Regulation by laying down minimum shares of the abovementioned CRMs. The shares may differ across materials and may exclude certain products, and will consider a number of criteria.

- Requirements related to the recycled content of permanent magnets that are set out in other Union legislation, e.g., the new Eco-design regulations, shall supersede requirements in this Article.

- The Article sets out further requirements to provide customers with the necessary information and to avoid misleading of confusing customers regarding magnetic products, including for distance selling, commercial activity and placing on the market.

- Products primarily designed for defence or space application will be exempt from these requirements.

- The requirements under this Article will apply to magnetic resonance imaging devices, motor vehicles and light means of transport that are type-approved vehicles of category L no sooner than five years from entry into force of the Regulation.

- The set-out requirements will not apply to certain special purpose vehicles, certain vehicle parts type-approved in multi-stage type approval of categories N1, N2, N3, M2 or M3, and certain vehicles produced in small series.

EU Cyber Resilience Act - UPDATE

What is the EU Cyber Resilience Act?

The EU Cyber Resilience Act (EU CRA) is an upcoming EU law designed to strengthen cybersecurity protections for consumers and businesses using products or software. It will enforce mandatory cybersecurity requirements.

The EU CRA is similar to the UK's Product Security and Telecommunications Infrastructure regime that began in April 2024, but it is broader and more comprehensive.

What products does the EU CRA apply to?

- Products with digital elements (PDEs) meaning software or hardware products.
- A PDE's remote data processing solutions.
- A PDE's software or hardware components that are placed on the market separately.

PDEs (products with digital elements) include a wide range of items such as smart household devices, toys, wearables, and software products. Certain categories, like medical devices, automotive vehicles, and aviation products, are exempt from the EU CRA's requirements due to existing regulations, with the possibility of future additions to the exempt list.

Who has obligations under the EU CRA, and what are the key obligations?

Obligations will be imposed on:

- *Manufacturers* (This includes anyone who designs, develops, or manufactures a PDE and markets it under their own name or trademark)
- An *appointed authorised representative* for a manufacturer.
- *EU-based importers* who place PDE's with the name/trademark of a non-EU-based person on the EU market.
- *Distributors*

The key obligations are to:

- Assess and mitigate cybersecurity risks during PDE design, development, and production.
- Ensure third-party components do not compromise PDE security.
- Document cybersecurity issues, including vulnerabilities and third-party information.
- Provide timely updates to fix or mitigate vulnerabilities.
- Offer security support for the shorter of the PDE's expected lifetime or five years after market release.

- Notify ENISA within 24 hours of discovering an exploited vulnerability or security incident and inform users of corrective measures.
- Provide information with PDEs, including manufacturer details, a contact for reporting vulnerabilities, instructions for installing updates, and secure decommissioning guidance.
- Establish a conformity assessment process to ensure compliance with the EU CRA.

These obligations mainly fall on manufacturers, but all supply-chain participants must ensure their products comply with the requirements. Importers, for example, must ensure they only place compliant PDEs on the EU market and that manufacturers have proper vulnerability handling processes.

What are the essential cyber security requirements?

The EU CRA's *essential cybersecurity requirements (ECRs)* are outlined in Annex I and focus on outcomes rather than specific technical details to stay future proof. They require PDEs to:

- Be designed, developed, and produced to ensure a high level of cybersecurity and minimize the impact of incidents.
- Be delivered without known exploitable vulnerabilities and with secure default settings.
- Protect against unauthorized access with appropriate control mechanisms.
- Safeguard the confidentiality of data through state-of-the-art encryption.
- Process only the data necessary for their intended use, adhering to data minimization principles.
- Limit attack surfaces, including external interfaces.
- Address vulnerabilities through security updates, including automatic updates and user notifications.

The EU CRA categorizes PDEs by risk. PDEs without critical cybersecurity risks fall into the 'default' category and can be self-assessed by their manufacturer. 'Critical' PDEs, classified as Class I and Class II, face stricter requirements and may need third-party conformity assessments.

The EU CRA mandates several *vulnerability handling requirements (VHRs),* including:

- Identifying and documenting vulnerabilities and components in a PDE.
- Regularly testing and reviewing a PDE's security.
- Implementing a vulnerability disclosure policy.
- Distributing patches and updates promptly and for free, along with user advice on necessary actions.

When will the Act take effect & what are the penalties for non-compliance?

The EU CRA was approved by the EU Parliament on 12 March 2024 and awaits formal adoption by the EU Council, expected later in 2024. After it becomes law, manufacturers, importers, and distributors will have 36 months to comply with most requirements, except for a 21-month grace period for manufacturers' reporting obligations on incidents and vulnerabilities.

Penalties for non-compliance with the EU CRA can include fines up to €15 million or 2.5% of a company's total annual worldwide turnover, whichever is higher.

How will it impact UK and other non-EU companies and what should they do now?

The EU CRA will impact UK and other non-EU companies by requiring compliance for any PDEs sold in the EU market. Businesses should start identifying which products will be affected and ensure compliance with the EU CRA. This includes coordinating with suppliers and updating contracts to reflect the new requirements.

Contact

Archie Maxwell
MTA Operations and Technical Assistant
archie.maxwell@mta.org.uk
020 7298 6420