EXPLANATORY MEMORANDUM FOR EUROPEAN UNION LEGISLATION WITHIN THE SCOPE OF THE UK/EU WITHDRAWAL AGREEMENT AND THE WINDSOR FRAMEWORK

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

Submitted by the Department for Science, Innovation and Technology.

4th DECEMBER 2024

SUBJECT MATTER

1. On 20 November 2024, the EU adopted a regulation on horizontal cyber security requirements for products with digital elements (full text here). This regulation, the Cyber Resilience Act (CRA), sets minimum safety standards for all products with a digital element, aiming to harmonise cyber security requirements for these products across all member states. The CRA will enter into force on 10 December 2024, with substantive requirements phased in over the following three years.

2. Once it comes into force, Articles 66 and 68 of the CRA will amend two pieces of EU legislation which are listed in Annex II of the Windsor Framework and therefore apply in Northern Ireland. Article 66 of the CRA will amend Regulation (EU) 2019/1020 relating to market surveillance. Article 68 of the CRA will amend Regulation (EU) 168/2013 relating to two- and three-wheel vehicles.

3. Any application of these pieces of legislation in Northern Ireland, as amended by Articles 66 and 68 of the CRA, would therefore be subject to the democratic scrutiny process set out in Schedule 6B to the Northern Ireland Act 1998 and Article 13(3a) of the Windsor Framework. The amendments to both Regulation (EU) 2019/1020 and Regulation (EU) 168/2013 are expected to have limited practical impact in isolation.

4. The remaining provisions of the CRA are freestanding rather than amending or replacing provisions already listed in Annex II of the Windsor Framework, and therefore would not apply to Northern Ireland under Article 13(3). As such, they would only be subject to the Windsor Framework's Article 13(4) process should they be notified formally in that regard by the European Commission. However, in the event of such a notification, further articles would only apply with the agreement of the UK and the EU at the Withdrawal Agreement Joint Committee, subject to democratic safeguards set out under Schedule 6B to the Northern Ireland Act 1998.

5. As a whole, the CRA will primarily impose obligations on the manufacturers of products with a digital element.[1] However, other supply-chain participants – such as importers and distributors – are required to ensure that any products with digital elements they place on the EU market comply with CRA requirements and that the manufacturer has compliant vulnerability handling processes in place.

6. Products with digital elements are defined in the CRA as being software and hardware products and their remote data processing solutions as well as their software and hardware components that are placed on the market separately.

7. The key obligations of the CRA on manufacturers include:
    i. manufacture products with digital elements that comply with the cybersecurity requirements set out in Part I of Annex I of the CRA
    ii. undertake a cyber security risk assessment, and ensure that the outcome is documented, considered in the planning, design, development, production, delivery and maintenance phases of the product with a digital element and is kept up to date
    iii. exercise due diligence when integrating components sourced from third parties[2]
    iv. document, in a manner that is proportionate to the risks, relevant revealed cyber security aspects, including vulnerabilities
    v. ensure that vulnerabilities are handled effectively[3]
    vi. provide security support for a product with a digital element's expected lifetime or for five years after a product with a digital element is placed on the market, whichever is shorter
    vii. ensure that the EU Agency for Cybersecurity (ENISA) is notified and that the product with a digital element's users are informed of corrective measures within 24 hours of being made aware of an actively exploited product with a digital element's vulnerability or an incident that might impact a product with a digital element's security
    viii. ensure that products with a digital element are accompanied by information,[4] and
    ix. establish a conformity assessment process.

8. New obligations will also be placed on member states. These include:

---

[1] "Manufacturers" is defined as anyone who designs, develops or manufactures a product with a digital element (PDE) and who markets the PDE under their name or trademark.
[2] Which includes free and open-source software components. The CRA states that the Commission may establish voluntary security attestation programmes to help users of these products assess their conformity.
[3] For instance, by providing updates for PDEs to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner.
[4] Such as the manufacturer's details and point of contact for reporting vulnerabilities.

i. designating one or more market surveillance authorities to oversee effective implementation of the CRA and ensuring they have sufficient resources
ii. ensuring enough notified bodies to carry out conformity assessments within 24 months of the CRA entering into force
iii. designating a notifying authority that will be responsible for creating and implementing procedures to assess and notify conformity assessment bodies, and
iv. ensuring an appeal procedure against decisions of the notified bodies is available.

9. The CRA categorises products with a digital element by risk. Products with a digital element are categorised into 'default', 'important', or 'critical' categories. All products with a digital element are required to go through a conformity assessment process. The nature of this process is differentiated by product category ('default', 'important', or 'critical') and set out in Article 32 of the Regulation, and additionally subject to Article 8 for 'critical' products.

10. While some aspects of enforcement are left to member state discretion, the CRA mandates varying levels of the maximum fines that can be imposed depending on the category of non-compliance (see Article 64).

11. Several product categories, which are seen as sufficiently regulated already, are exempt from CRA requirements, for instance, medical devices and motor vehicles. In addition, only software developed for commercial purposes is in scope of the CRA. The development of products with digital elements that are free qualifying as free and open-source software by not-for-profit organisations should not be considered to be a commercial activity for the purposes of the CRA.[5] The CRA also does not apply to people who contribute with source code to a product with digital elements qualifying as free and open-source software that are not under their responsibility.[6] The CRA also places more limited rules on open-source software developers regarding documentation and vulnerability handling.

SCRUTINY HISTORY

12. Below are details of Explanatory Memoranda that have a relationship to this regulation:

    a. DCMS published an Explanatory Memorandum (COM/2022/454) for "European Union legislation within the scope of the UK/EU Withdrawal Agreement and Northern Ireland Protocol" on the CRA proposal in December 2022.

[5] Recital 18 of the preamble.
[6] Recital 18 of the preamble.

b. The European Scrutiny Committee provided its reflections on this Explanatory Memorandum in its Seventeenth Report, published in April 2023.

MINISTERIAL RESPONSIBILITY

13. The Secretary of State for Science, Innovation and Technology has responsibility for cyber security policy in relation to the UK economy.

14. The Secretary of State for Business and Trade has responsibility for product safety as well as the UK internal market.

INTEREST OF THE DEVOLVED ADMINISTRATIONS

15. Cyber security remains a high interest subject area across the UK and Devolved Administrations.[7] We expect engagement between the Devolved Administrations and the UK Government to continue, to address UK-wide challenges and to realise UK-wide opportunities.

LEGAL AND PROCEDURAL ISSUES

Legal Basis

16. Article 114 of the Treaty on the Functioning of the European Union (TFEU), which allows for the adoption of measures to ensure the establishment and functioning of the internal market.

Voting Procedure

17. Qualified Majority Voting.

Timetable for adoption and implementation

18. The legislation will be implemented in phases:
    a) 20 days after the date of publication: The CRA enters into force.
    b) 18 months after the date of entry into force: Chapter IV (Articles 35 to 51), setting down rules for the notification of conformity assessment bodies, becomes applicable.
    c) 21 months after the date of entry into force: Article 14, on reporting obligations of manufacturers, becomes applicable.
    d) 36 months after entry into force: All CRA requirements are applicable.

[7] As evidenced, for instance, in the Scottish Government's "Taking Stock: report on progress towards a cyber resilient Scotland" (2023) report.

POLICY AND LEGAL IMPLICATIONS

Domestic Policy Context

19. The UK has its own regulatory regime for product security, the Product Security and Telecommunications Infrastructure (PSTI) Act 2022 and associated Regulations, which entered into force in April 2024 and covers UK consumer connectable products.[8] The Act creates powers for ministers to specify security requirements relating to consumer connectable products. Manufacturers involved in making these products available to UK customers now need to comply with three baseline security requirements (around avoiding default passwords, around providing information on how to report security issues, and around providing information on minimum security update periods) set out in the Act. In addition to the PSTI regime, DSIT is currently approaching software security through non-legislative levers. It is drafting a voluntary Code of Practice for Software Vendors, focused on improving the resilience and security of software in the UK, and it has recently closed a call for Views on this draft Code.

20. While the substantive requirements of the CRA will not apply to the UK, it may have implications for UK manufacturers and software/app/open-source developers whose products are sold, imported, distributed and/or used in the EU single market.

21. Overall, the UK Government recognises the need to improve cyber security which we are tackling at an international level with the EU, as well as domestically. We are broadly aligned on the policy goals described here and therefore manufacturers are already taking action to address these across the UK and the EU.

Potential impact of the CRA in Northern Ireland

22. The CRA makes a consequential amendment to Regulation (EU) 2019/1020 on Market Surveillance and Product Compliance (MSC),[9] which applies in Northern Ireland. This amendment interacts with the substantive provisions of the CRA which will not apply in Northern Ireland under Article 13(3) of the Windsor Framework. Those measures, if applied, would set out the requirements against which compliance would be assessed under market surveillance measures. However, in the absence of those requirements, this amendment in isolation is considered to have limited practical effect.

---

[8] Certain categories of consumer connected products can be excluded from the PSTI's scope if they are or will soon be covered by equal or greater security requirements. For instance, DSIT intends to exempt categories of 'automotive vehicles' from the PSTI's scope via a statutory instrument, subject to Parliamentary time.

[9] Namely, the CRA will be added to Annex 1 of MSC.

23. The CRA also amends Regulation (EU) 168/2013 on the Approval and Market Surveillance of Two- or Three-Wheel Vehicles and Quadricycles (known as L category vehicles), which applies in Northern Ireland. The amendment updates the table of technical requirements applicable under the framework to add an entry for 'protection of vehicle against cyberattacks'. Unlike other amendments, this amendment does not reference the CRA, so it appears to be an administrative update with reference to technical requirements to follow. Accordingly, this amendment in isolation will also have no practical effect.

Prior engagement with the EU

24. DSIT and DG CNCT[10] officials discussed their respective policies for secure technology and 'secure by design' approaches at the EU-UK Cyber Dialogue in December 2023. During that discussion, officials spoke about the necessity of internationally recognised standards in a global marketplace.

CONSULTATION

25. The EU Commission ran a public consultation from 16 March 2022 to 25 May 2022 in preparation of the Act. A total of 167 valid responses were submitted, with only one response from the UK.

FINANCIAL IMPLICATIONS

26. Given the provisions falling under Article 13(3) are expected to have limited (if any) impact, no financial implications are expected by virtue of those provisions – save the cost of potential trade frictions that all UK businesses trading with the EU may face.

Feryal Clark MP
Parliamentary Under Secretary of State at the
Department for Science, Innovation &Technology

[10] The EU Directorate-General for Communications Networks, Content and Technology.