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

Council Decision (EU) 2025/799 of 14 April 2025 establishing the position to be taken on behalf of the European Union within the Joint Committee established by the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community as regards the adoption of a decision adding a newly adopted Union act to Annex 2 to the Windsor Framework

Submitted by the Department for Science, Innovation and Technology.

5 May 2026

SUBJECT MATTER

1. Council Decision (EU) 2025/799 is a non-legislative act, which empowers the European Commission, on behalf of the European Union, to take a position at the Withdrawal Agreement Joint Committee (the 'Joint Committee') in respect of Regulation (EU) 2024/2847 on cyber resilience[1] (Cyber Resilience Act or 'CRA'). The position is that Regulation (EU) 2024/2847:

    i. both neither amends nor replaces acts listed in the Annexes to the Windsor Framework, with the exception of Articles 66 & 68 and;

    ii. falls within the scope of the Windsor Framework, with the exception of Articles 5 & 67 and should be added to point 47 of Annex 2 of the Windsor Framework.

2. Any application of these elements under the Windsor Framework can only take place following a joint decision between the UK and EU at the Joint Committee, in line with Article 13(4). Any decision on the UK's part to agree to add these elements to the Framework can only take place subject to democratic safeguards set out under Schedule 6B to the Northern Ireland Act 1998.

3. The Cyber Resilience Act sets minimum safety standards for all products with digital elements, aiming to harmonise cyber security requirements for these products across all member states. The CRA entered into force on 10 December 2024, with substantive requirements set to phase in over the following three years.

[1] 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)

4. Articles 66 and 68 of the CRA amend two pieces of EU legislation which are listed in Annex 2 of the Windsor Framework and therefore apply in Northern Ireland. Article 66 of the CRA amends Regulation (EU) 2019/1020 which relates to market surveillance, extending market surveillance measures and powers to the CRA; Article 68 of the CRA amends Regulation (EU) 168/2013 which relates to two- and three-wheel vehicles and quadricycles, and adds a requirement of 'protection of vehicle against cyberattacks' to this regulation. The amendments to both Regulation (EU) 2019/1020 and Regulation (EU) 168/2013 are expected to have limited practical impact in isolation and are applied to Northern Ireland through Article 13(3) of the Windsor Framework.

5. The CRA will primarily impose obligations on the manufacturers of products with digital elements.[2] However, other supply-chain participants – such as importers and distributors – also have obligations under the CRA. For example, they are required to ensure that any products with digital elements they place on the EU market comply with CRA requirements and must inform manufacturers of any vulnerabilities or risks, where they become aware of any. Products with digital elements are defined in the CRA as being software and hardware products and their remote data processing solutions.

6. 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[3]
    iv. document, in a manner that is proportionate to the risks, relevant cyber security aspects, including vulnerabilities
    v. ensure that vulnerabilities are handled effectively[4]
    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 digital elements 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

[2] "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.

[3] 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.

[4] For instance, by providing updates for PDEs to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner.

viii. ensure that products with digital elements are accompanied by required information,[5] and
ix. establish a conformity assessment process and affix the CE mark.

7. New obligations will also be placed on Member States. These include:
   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.

8. The CRA categorises products with digital elements by risk. All products in scope must meet the basic requirements, but some products with digital elements are categorised as 'important' or 'critical'. The main difference between 'important' and 'critical', and all other products, is the required conformity process. All products with a digital element are required to go through a conformity assessment process. While standard products allow for self-assessment, important products require third-party assessment unless specific harmonised standards are followed (for some lower-risk important products). Critical products must always undergo third-party conformity assessment. The nature of this process is differentiated by product category (standard/unclassified, 'important', or 'critical') and set out in Article 32 of the Regulation, and additionally subject to Article 7 for 'important' products and Article 8 for 'critical' products.

9. 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).

10. Several product categories, which are seen as sufficiently regulated already, are exempt from CRA requirements, for instance, medical devices and motor vehicles. The development of products with digital elements that are free or qualifying as free and open-source software by not-for-profit organisations, should not be considered to be[6]. 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.[7] The CRA also places more limited rules on open-source software developers regarding documentation and vulnerability handling.

[5] Such as the manufacturer's details and point of contact for reporting vulnerabilities.

[6] Recital 18 of the preamble.

[7] Recital 18 of the preamble.

SCRUTINY HISTORY

11. Below are details of Explanatory Memoranda that have a relationship to this decision:

    a. The Department for Digital, Culture, Media & Sport 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.
    b. The European Scrutiny Committee provided its reflections on this Explanatory Memorandum in its Seventeenth Report, published in April 2023.
    c. The Department for Science, Innovation and Technology published an Explanatory Memorandum covering the elements of the CRA applicable to Northern Ireland under Article 13(3) of the Windsor Framework in December 2024.

MINISTERIAL RESPONSIBILITY

12. The Minister for the Cabinet Office has responsibility for making decisions for the UK Government at the Withdrawal Agreement Joint Committee.

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 GOVERNMENTS

15. Cyber security remains a high interest subject area across the UK and devolved administrations.[8] 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

EU Legal Basis

16. Article 218(9) of the Treaty on the Functioning of the European Union enables the European Council, on a proposal from the European Commission to adopt a

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

decision establishing the positions to be adopted on the EU's behalf in a body set up by an agreement.

Voting Procedure

17. Qualified Majority Voting.

POLICY AND LEGAL IMPLICATIONS

18. Council Decision (EU) 2025/799 provides the legal basis for the EU to take a position at the Joint Committee on adding the majority of articles in Regulation 2024/2847 to Annex 2 of the Windsor Framework under Article 13(4). If the position within the Council Decision were to be adopted as a Joint Decision at a meeting of the Joint Committee, those articles would then be applicable in Northern Ireland, as is the case within EU Member States. Those articles would be applied alongside Articles 66 & 68, which are already applicable under Article 13(3) of the Windsor Framework.

19. Under Section 15(C) of the European Union (Withdrawal) Act 2018, no decision may be made at the Joint Committee by a UK Minister via the written procedure process provided for in Rule 9(1) of Annex VIII of the withdrawal agreement. As such any agreement to adopt this decision could only take place following a meeting of the Joint Committee.

20. Under Schedule 6B to the Northern Ireland Act 1998, UK Ministers cannot agree to add a new EU act to the Windsor Framework unless the NI Assembly has passed an "applicability motion" with cross-community consent. Ministers can also agree to add a new EU act if they consider that the act in question would not create a new regulatory border between Great Britain and Northern Ireland, or in exceptional circumstances.

21. Under Article 13(4) of the Windsor Framework, the UK requested an exchange of views to better understand the application and impacts of the CRA, should it be added to Annex 2. This exchange of views is focussed on assessing whether any new EU acts added to the Framework are necessary for its proper functioning. The UK Government is looking into how the arrangements would interact with the avoidance of a hard border on the island of Ireland, and, as the CRA involves the regulation of products with digital elements, the relationship between these products, the movement of goods and the unique circumstances of Northern Ireland.

22. This exchange of views between the UK and EU remains ongoing. The UK aims to ensure that any application of the Act is proportionate and appropriate within the specific context of the Windsor Framework. Once these have concluded, any

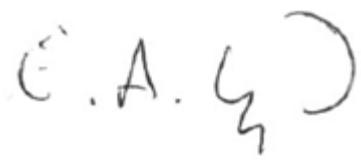
decision to apply the substantive elements of the CRA through Article 13(4) would still require agreement from the UK, subject to domestic law.

CONSULTATION

23. No consultation has been undertaken as this Council Decision will have no direct effect on the UK or specifically on Northern Ireland unless the UK agrees to add the Cyber Resilience Act to the Framework.

FINANCIAL IMPLICATIONS

24. Not applicable



Baroness Lloyd of Effra CBE

Parliamentary Under Secretary of State for Digital Economy
Department for Science, Innovation and Technology