EXPLANATORY MEMORANDUM FOR EUROPEAN UNION LEGISLATION WITHIN THE SCOPE OF THE UK/EU WITHDRAWAL AGREEMENT AND NORTHERN IRELAND PROTOCOL

COM/2022/454 final

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

Submitted by the Department for Digital, Culture, Media & Sport

20/12/22

SUBJECT MATTER

1. The European Union (EU) has proposed a new Regulation on horizontal cyber security requirements for products with digital elements (known as the "Cyber Resilience Act". The stated purpose of the proposed Regulation is to harmonise cyber security requirements for products with digital elements in all Member States, and to remove obstacles to the free movement of goods.

2. Broadly, the provisions capture all hardware and software products in its definition of "products with digital elements", where the security of these products is not otherwise captured by existing EU legislation. For instance, the security of both hardware and software medical products is already regulated under EU Regulations 2017/745, and 2017/746.

3. Two main objectives cited by the EU for its proposal are:
    a. to create conditions for the development of secure hardware and software products by ensuring they are placed on the market with fewer vulnerabilities, and ensuring that manufacturers take security seriously through a product's life cycle; and
    b. to create conditions allowing users to take cyber security into account when selecting and using products with digital elements.

4. The EU cites a number of high profile cyberattacks resulting from suboptimal product security as justification for this intervention, including the WannaCry ransomware worm, which exploited a Windows vulnerability that affected 200,000 computers across 15 countries in 2017.

5. Key measures in the Regulation include an obligation on manufacturers of products with digital elements to undertake an assessment of the cyber security

risks associated with those products, and to comply with essential cybersecurity requirements on the basis of that risk assessment. Manufacturers would also be required to report actively exploited vulnerabilities, and incidents having impact on the security of a product, to the European Union Agency for Cybersecurity (ENISA).

6. Additionally, the Regulation would oblige manufacturers to comply with minimum vulnerability handling requirements for the expected product lifetime, or five years from the point where the product is placed on the market, whichever is shorter.

SCRUTINY HISTORY

7. REGULATION (EU) 2019/1020 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 was subject to scrutiny as EU document 15950/17, COM(17)795. BEIS submitted an EM dated 12 January 2018.

8. The House of Commons European Scrutiny committee reported that the proposal raised issues of political importance and completed scrutiny on 4 September 2019 in Report 73, 17/19. The proposal was examined by the House of Lords European Union Committee's Internal market Sub-Committee and scrutiny was completed on 16 January 2020.

INTEREST OF THE DEVOLVED ADMINISTRATIONS

9. As a newly proposed legislative intervention, the proposed Regulation is not listed in Annex 2 of the Northern Ireland Protocol, nor is there any Regulation mandating minimum cyber security requirements for all products with digital elements in Annex 2. Therefore, the proposed cyber security regulatory framework set out in the Regulation would not apply in Northern Ireland under article 5(4) of the Protocol.

10. The Protocol provides that the cyber security of products with digital elements are to be governed by the law of the United Kingdom, as per article 7(1), subject to Articles 34 and 36 of the Treaty on the Functioning of the European Union (“TFEU”).

11. The government considers that the matters to which the proposal relates are reserved:

    a. Product safety, and telecommunications and wireless telegraphy, are reserved matters under C8 and C10 of Schedule 5 to the Scotland Act 1998.

b. Consumer safety, and telecommunications, are listed as reservations under s29 and s37 of Schedule 3 of the Northern Ireland Act 1998.

c. Product safety, and telecommunications and wireless telegraphy, are reserved matters under C7 and C9 of Schedule 7 of the Government of Wales Act 2006.

12. Officials from the Northern Ireland Executive with an interest in this proposal were consulted in drafting this explanatory memorandum.

LEGAL AND PROCEDURAL ISSUES

Legal Basis

13. The legal basis for the proposed Regulation is Article 114 TFEU. There is no legal basis for the proposed Regulation to have effect in the UK.

Timetable for adoption and implementation

14. Given that the draft Regulation is at the proposal stage, and has not yet cleared the EU legislative scrutiny processes, it is unclear when these measures will come into effect in the EU.

15. The EU has indicated, however, that the proposed Regulation will become applicable 24 months after its entry into force, with the exception of the reporting obligations on manufacturers set out in Article 11, which will apply 12 months after its entry into force. It is therefore likely that the Regulation will not become applicable in its entirety, in Member States, until 2025 at the earliest.

POLICY IMPLICATIONS

16. As set out in paragraph 9 above, the proposed Regulation is not listed in Annex 2 of the Northern Ireland Protocol, and will therefore not be applicable in respect of Northern Ireland, other than in respect of a technical matter set out below.

17. The proposed Regulation would amend Regulation (EU) 2019/1020 on market surveillance and compliance of products, so that the new proposed Regulation is added to the List of *"Union harmonised legislation"* in Annex 1 of the 2019/1020 Regulation. Regulation 2019/1020 is not directly included within Annex 2 of the Northern Ireland Protocol, but Regulation 2019/1020 does apply in Northern Ireland by operation of Regulation 765/2008, which is specified in Annex 2 of the Protocol.

18. Market surveillance authorities monitor and, where appropriate, enforce the requirements of European product safety law, using the powers and enforcement tools provided by UK law. Different authorities, such as the Health

and Safety Executive for Northern Ireland, enforce different aspects of product safety legislation. Regulation 2019/1020 harmonises requirements for market surveillance authorities and applies to all legislation listed in Annex 1 of the Regulation. By adding the new Regulation to the Annex, economic operators making products with digital elements available to customers in Northern Ireland could be subject to the obligation to cooperate with market surveillance authorities regarding actions which could eliminate or mitigate risks presented by their products. The market surveillance authorities appointed by the UK government with respect to Northern Ireland could also be legally obligated to provide economic operators with information concerning the implementation of the proposed Regulation applicable to their products. The government's view, however, is that because the proposed Regulation has no effect in the UK including in Northern Ireland, then any consequential changes to other legislation that does apply in Northern Ireland, cannot have effect.

19. Whilst the UK government deeply values the benefits that technology and greater connectedness can bring to our economy and society, we recognise that action needs to be taken to assess and address the risks to individuals, businesses, and the wider economy, that vulnerabilities in hardware and software products represent.

20. As the EU acknowledges, in empowering hardware manufacturers and software developers to make their own determinations about the risk profile presented by their products, the cyber security risks posed by different digital product categories is highly variable. The proportionality of implementing a given security measure in relation to a product will depend on myriad factors, from the architecture of the product, to the data it processes, to the setting in which it is ultimately deployed. Consequently, a one-size-fits-all approach to regulating product security risks imposing obligations on businesses that are disproportionate to the associated security benefits.

21. The UK government recognises that inadequately targeted security regulation could risk stifling digital innovation. That is why my department is taking forward a body of work, set out in the National Cyber Strategy, to assess the case for targeted regulatory interventions that recognise the heterogeneous risk profiles posed by different digital products categories.

22. The Product Security and Telecommunications Infrastructure (PSTI) Act 2022 enables the specification of mandatory minimum security requirements for consumer connectable products. The requirements of this legislation apply UK-wide, and will enable the imposition of a security baseline. This security baseline will initially be based on key provisions from the leading global standard for consumer device security, European Telecommunications

Standards Institute (ETSI) ETSI EN 303 645. This intervention has been widely welcomed by industry, cybersecurity experts, and consumer rights bodies.

23. The PSTI Act empowers the UK government to introduce further requirements that businesses in the supply chain of consumer connectable products will need to comply with, including requirements in respect to software related to the physical device, business process requirements, and requirements for businesses to supply customers with security information in respect to consumer connectable products.

24. We are also actively assessing the case for regulatory and non-regulatory interventions in respect of other digital product categories. In May 2022, the government published draft security principles for manufacturers of enterprise-connected devices. In that same month, we also launched a call for views on a voluntary Code of Practice for App Store Operators and Developers, and published the Code of Practice on 9 December 2022. We are also delivering a comprehensive programme of work to support the cyber security of the UK's connected places, including the publication of Connected Places Cyber Security Principles for those designing, building and operating connected places.

CONSULTATION

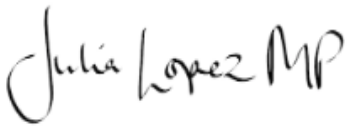
25. The European Commission conducted an impact assessment for the proposed Regulation between 16 March 2022 and 25 May 2022. As the proposal Regulation will not be applicable in Northern Ireland, the UK government has no plans to consult on this matter.

FINANCIAL IMPLICATIONS

26. When it becomes applicable, the proposed Regulation may have a financial impact on UK businesses placing products with digital elements on the EU market. Software developers and hardware manufacturers may incur costs from new cyber security requirements, conformity assessment, as well as documentation and reporting obligations. Importers and Distributors may also incur familiarisation and verification costs as a result of the proposal.

27. The anticipated costs to businesses could not be estimated in the EU impact assessment, including familiarisation costs, and costs related to information and transparency requirements. The impact on UK businesses in respect of consumer products may depend on whether the implementation of the new Regulation aligns with the security requirements that will be implemented in the UK under PSTI Act powers.

MINISTERIAL NAME AND SIGNATURE



Julia Lopez

Minister of State for Media, Data and Digital Infrastructure

Department for Digital, Culture, Media & Sport