CLIFFORD

CHANCE

EU CYBER RESILIENCE ACT – PROPOSED CYBERSECURITY RULES FOR CONNECTED PRODUCTS

EU CYBER RESILIENCE ACT – PROPOSED CYBERSECURITY RULES FOR CONNECTED PRODUCTS

The **proposed Cyber Resilience Act** will introduce new common cybersecurity requirements for "products with digital elements" placed on the EU market. Forming part of the EU's Cybersecurity Strategy, this proposed regulation would impose a range of obligations on manufacturers, importers and distributors of connected hardware and software, with the aim of ensuring that technical vulnerabilities are minimised and managed in a transparent manner. This briefing discusses key aspects of the proposal.

WHAT IS THE CYBER RESILIENCE ACT (CRA)?

On 15 September 2022 the European Commission (the **Commission**) published its proposal for a regulation on horizonal cybersecurity requirements for products with digital elements (the **Cyber Resilience Act** or **CRA**).

The CRA aims to create a framework for the development of secure products with digital elements, and for ensuring security is managed throughout their life cycle. It would also ensure purchasers and users have sufficient information about cybersecurity in relation to such products.

WHAT IS THE SCOPE OF THE CRA?

Products in scope

The CRA proposes to introduce cybersecurity-related obligations for manufacturers, importers and distributors of any software or hardware and their remote data processing solutions – called "products with digital elements" or **PDEs** – whose intended or foreseeable use includes a data connection to a device or a network. The CRA also covers any non-embedded software or hardware components that are sold separately from a PDE. This broad scope has the effect of capturing: (i) any software and hardware connected to the Internet; (ii) any related software that is needed for those connected products to operate; and (iii) any components that are intended to be integrated into such products.

While the territorial scope of application is not specifically set out in the current proposal, various references to PDEs being "placed on the EU market" or "made available on the market" suggest that the CRA will apply to any PDEs offered for sale or use in the EU.

Exceptions

The CRA explicitly excludes medical and in-vitro medical-diagnostic devices as well as motor vehicles, which are already subject to sector-specific regulations, as well as PDEs developed exclusively for national security or military purposes, or products

specifically designed to process classified information. The Commission would be able to pass secondary legislation to limit or exclude the application of the CRA to PDEs covered by other EU rules in certain circumstances provided the sectoral rules achieve the same level of protection.

KEY OBLIGATIONS FOR MANUFACTURERS

Cybersecurity by design and risk assessments

Manufacturers would be required to assess the cybersecurity risks associated with the PDE and take the outcome into account during the planning, design, development, production, delivery and maintenance phases of the PDE's life cycle, with a view to minimising cybersecurity risks, preventing security incidents and minimising the impact of such incidents. A cybersecurity risk assessment would need to be included in technical documentation when a PDE is placed on the EU market and be updated if vulnerabilities are later identified.

There are also due diligence obligations proposed for manufacturers when sourcing third-party components for PDEs, to ensure such components do not compromise the cybersecurity of the product.

In particular, manufacturers would be required to ensure that PDEs placed on the EU market fulfil certain cybersecurity requirements (**essential requirements**) set out in Annex I to the CRA. These include:

- protecting against unauthorised data access, modification or manipulation, and reporting on data corruption;
- designing, developing and producing the product to limit attack surfaces, reduce the impact of any incidents through exploitation mitigation mechanisms, and minimise negative impacts on the availability of services provided by other devices or networks;
- adopting the principle of data minimisation;
- including a 'secure by default' configuration, with the option to reset the product to this original state; and
- ensuring vulnerabilities can be easily addressed through security updates.

Conformity assessments

Manufacturers would be required to conduct assessments of whether the essential requirements have been fulfilled in relation to the PDE and that the manufacturer meets the vulnerability handling requirements (conformity assessments), except in limited cases where a presumption of conformity exists.

For lower-risk PDEs (i.e., those in the "default category"), the conformity assessment procedure may involve a self-assessment by a manufacturer using one of the methods prescribed under the CRA. However, PDEs that are considered "critical products" (subdivided into “Class I” and “Class II”) due to the risk profile associated with their functionality and intended use, are subject to additional requirements in relation to

conformity assessments (which, in the case of Class II critical products, would include the involvement of an authorised third party).

- **Examples of 'default category' products** include photo editing, word processing, smart speakers, games and hard drives.
- **Examples of Class I critical products** include identity management systems software, standalone and embedded browsers, password managers, network interfaces, firewalls and microcontrollers.
- **Examples of Class II (higher risk) critical products** include operating systems for servers, desktops and mobile devices, public key infrastructure and digital certificate issuers, industrial firewalls, CPUs and secure elements.

Manufacturers would need to be able provide all information and documentation necessary to demonstrate conformity of the PDE with the requirements under the conformity assessment regime upon request of a market surveillance authority.

Once compliance with the conformity assessment procedure has been demonstrated, manufacturers would be required to draw up an EU declaration of conformity which must include, among other things, the name, type and any additional information enabling the unique identification of the PDE, and the name and address of the manufacturer. This EU declaration of conformity would need to be provided with the PDE, or an internet address where the declaration can be accessed would need to be provided in the instructions to the user.

For the expected product lifetime or for the period of five years from the placing of the PDE on the market (whichever is shorter) manufacturers who know or have reason to believe that a PDE or the manufacturer's vulnerability handling processes are not in conformity with the essential requirements set out in the CRA would be required to immediately take corrective measures to bring the product or processes into conformity, or to withdraw or recall the product.

Managing vulnerabilities

For the expected product lifetime or for the period of five years from the placing of the PDE on the market (whichever is shorter) manufacturers would be required to ensure product vulnerabilities are handled effectively. This includes:

- identifying and document vulnerabilities;
- applying effective regular testing, and addressing and remediating vulnerabilities without delay;
- providing security updates in a timely manner and security patches free and without delay to address identified security issues (and providing associated information); and
- providing a contact address for the reporting of vulnerabilities and enforcing a co-ordinated vulnerability disclosure policy to process and remediate vulnerabilities.

Incident reporting

If a manufacturer becomes aware of any actively exploited vulnerability contained in the product, or of any incident having an impact on the security of the product, it must notify the EU Agency for Cybersecurity (**ENISA**) without undue delay and in any event within 24 hours. The CRA defines an "actively exploited vulnerability" as "a vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner".

ENISA will notify the Computer Security Incident Response Team of any actively exploited vulnerability, or the relevant single point of contact in each Member State of any incident impacting the security of a PDE, as well as inform the market surveillance authorities.

Manufacturers would also be required to inform the PDE's users without undue delay of an incident and any corrective measures that they might deploy.

Technical documentation

Manufacturers would be required to draw up technical documentation, which must contain all relevant data of the means used by the manufacturer to ensure the PDE and the processes put in place by the manufacturer comply with the essential requirements of the CRA before the PDE is placed on the market. This includes a description of the design, development and production of the PDE and vulnerability handling processes, the cybersecurity risk assessment, vulnerability tests and handling processes, and a copy of the EU declaration of conformity.

This technical documentation would need to be continuously updated during the expected product lifetime or during a period of five years after placing on the market (whichever is shorter). It would also need to be kept at the disposal of the market surveillance authorities for 10 years after the PDE has been placed on the market.

Appointed representatives

Manufacturers may appoint authorised representatives by a written mandate to perform specific tasks required by the CRA. The CRA specified certain tasks that must be permitted within an authorised representative's mandate (e.g., in relation to co-operation with market surveillance authorities) and excludes certain obligations from the mandate (e.g., responsibility for the cybersecurity risk assessment).

KEY OBLIGATIONS FOR IMPORTERS AND DISTRIBUTORS

The CRA also introduces due diligence obligations for importers and distributors of PDEs. In particular, before placing or making available a PDE on the EU market, importers and distributors would be required to ensure that the relevant conformity assessment has been carried out by the manufacturer (or, in the case of distributors, that a declaration of conformity has been provided or is available), that CE marking has been affixed (indicating that the product manufacturer has checked the product complies with EU requirements), and the PDE is accompanied by specific information, documentation and instructions.

Importers or distributors identifying a vulnerability in a PDE would be required to inform the manufacturer without undue delay. If an importer or distributor has reason to believe that a PDE presents a significant cybersecurity risk, it would be obliged to immediately inform the manufacturer and relevant market surveillance authorities.

Importers and distributors would also be subject to certain other reporting obligations, product recall and withdrawal measures, and record-keeping requirements.

MARKET SURVEILLANCE, ENFORCEMENT AND PENALTIES

Enforcement

Member States	EU level
Member States will each designate one or several 'market surveillance authorities' (**MSA**) to ensure the supervision and enforcement of the CRA at national level, including in relation to the evaluation of PDEs which present a significant cybersecurity risk, the issuance of guidance to operators, and the imposition of corrective or restrictive measures and penalties. For PDEs under the CRA that would also be classified as "high-risk AI systems" under the EU Artificial Intelligence Act, the national authorities responsible for market surveillance activities under the CRA and the Artificial Intelligence Regulation would be the same.	Unlike the EU General Data Protection Regulation and the EU Digital Services Act, the CRA does not establish a one-stop shop mechanism for cross-border infringements. However, it establishes an EU supervisory structure in the form of a dedicated co-operation group (**ADCO**) to ensure the uniform application of the CRA. This ADCO would be composed of the national MSAs and representatives of single liaison offices constituted under the EU Market Surveillance Regulation. Representatives from the Commission would also be included.
MSAs will have the power to access all data and related internal documentation that must be retained by organisations under the CRA (including information in respect to the design, development, and vulnerability handling of such products). Other EU authorities will also benefit: for instance, national data protection supervisory authorities have the right to access all documentation created to comply with the CRA, when such documentation is relevant for the fulfilment of their tasks, and MSAs would have an obligation to report any information of interest to the Commission and the relevant national competition authorities.	The Commission would have a central role and exclusive powers in the supervision and enforcement of the CRA, and responsibility in ensuring that decisions adopted by Member States in respect of the CRA are in line with EU law. In addition, the CRA proposal contains a "Union safeguard procedure" which allows the Commission to settle objections raised by Member States in relation to measures implemented by another Member State (including the prohibition or withdrawal of products by MSAs), with unlawful or unjustified measures being withdrawn and justified measures being adopted by all Member States.

Penalties and Sanctions

Depending on the nature of the violation, fines can range from EUR 5 – 15 million to 1 – 2.5% of worldwide turnover in the preceding financial year, whichever is higher.

- Breaches of the essential requirements, conformity assessment and reporting obligations may result in administrative fines of up to EUR 15 million or 2.5% of the annual global turnover, whichever is higher.
- Breaches of the other CRA rules, including obligations applicable to importers or distributors, may result in administrative fines of up to EUR 10 million or 2% of the annual global turnover, whichever is higher.
- Organisations which provide incorrect or misleading information face administrative fines of up to EUR 5 million or 1% of annual turnover.

Non-compliance with CRA requirements may also result in corrective or restrictive measures, including the MSA or the Commission recalling or withdrawing products from the EU market.

NEXT STEPS AND TRANSITIONAL PROVISIONS

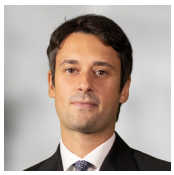
The draft of the CRA will now pass to the European Parliament and Council for adoption (and possible amendment) according to the ordinary legislative procedure. While it is difficult to predict the time required for Parliament and the Council to reach consensus, this often takes between 18 months and two to three years.

The Commission has proposed that the majority of the new rules should apply 24 months following the publication of the CRA in the Official Journal (with the exception of manufacturer reporting obligations for actively exploited vulnerabilities and incidents, which will apply 12 months after the CRA enters into force).

To aid a smooth transition between current EU legislation and the CRA, there is a proposed 42-month transition window for products that have already been approved. For products that have been placed on the marker prior to the CRA becoming law, they will not be subject to the requirements of the CRA, unless they undergo substantial modifications to their design or purpose.

Given that the Commission has proposed an EU Regulation (as opposed to a Directive), the CRA will be directly applicable once adopted, rather than dependent on individual Member States enacting national provisions to bring the CRA into force. It will be key, therefore, for affected businesses to be prepared in advance to comply with the obligations set out in the final form of the CRA.

AUTHORS



Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435t
E: andrea.tuninettiferrari@cliffordchance.com

Oscar Tang
Senior Associate
London
T: +44 207006 3749
E: oscar.tang@cliffordchance.com

Rita Flakoll
Senior Associate
Knowledge Lawyer
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

Alexandre Balducci
Associate
Paris
T: +33 1 4405 5137
E: alexandre.balducci@cliffordchance.com

Sonsoles Callejo
Abogado
Madrid
T: +34 91 590 4133
E: sonsoles.callejo@cliffordchance.com

Grégory Sroussi
Counsel
Paris
T: +33 1 4405 5248
E: gregory.sroussi@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

CONTACTS

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Samantha Ward
Partner
London
T: +44 207006 8546
E: samantha.ward@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

Carlos Zabala
Counsel
Madrid
T: +34 91 590 7515
E: carlos.zabala@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Andrei Mikes
Senior Associate
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Heiner Hugger
Partner
Frankfurt
T: +49 69 7199 1283
E: heiner.hugger@cliffordchance.com

Ines Keitel
Partner
Frankfurt
T: +49 69 7199 1250
E: ines.keitel@cliffordchance.com

David Pasewaldt
Partner
Frankfurt
T: +49 69 7199 1453
E: david.pasewaldt@cliffordchance.com

Charles-Henri Laevens
Senior Associate
Luxembourg
T: +352 48 50 50 485
E: charleshenri.laevens@cliffordchance.com

Zayed Al Jamil
Partner
London
T: +44 207006 3005
E: zayed.aljamil@cliffordchance.com

Gunnar Sachs
Partner
Düsseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Thomas Voland
Partner
Düsseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Chris Ireland, Maria Giulia Tammaro, Anna Pfister, Hari Pannum, Sanjay Shelat and Daniel Murray contributed to the drafting of this briefing.

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2211-003439