CLIFFORD

CHANCE

THE EU CYBER RESILIENCE ACT – TOWARDS A SAFE AND SECURE DIGITAL MARKET IN EUROPE

THE EU CYBER RESILIENCE ACT – TOWARDS A SAFE AND SECURE DIGITAL MARKET IN EUROPE

The EU's Cyber Resilience Act (**CRA**) is waiting in the wings. On Tuesday 12 March, the **European Parliament voted** to approve the text of this milestone EU regulation, reflecting the political agreement reached by the European Parliament and the Council of the European Union late last year. The CRA is now awaiting formal approval by the Council and is expected to enter into force in the coming months.

Originally proposed by the European Commission in September 2022, the CRA will introduce mandatory cybersecurity requirements for products with digital elements made available on the EU market, establishing a consistent EU-wide legal framework for essential cybersecurity requirements for such products.

In this briefing we overview **the CRA as adopted by the European Parliament on 12 March 2024**, including the obligations imposed on those involved in the supply chain of connected devices, and consider key changes made by the Council and the European Parliament (the co-legislators) to the European Commission's original proposal.

OVERVIEW

The CRA governs the cybersecurity of "*products with digital elements*" (**PDEs**), including any software, hardware or components thereof, made available on the EU market.

The CRA pursues four objectives:

1. ensuring cybersecurity standards for the design, development and production of PDEs throughout their life cycle;

2. ensuring a coherent cybersecurity framework for PDEs across the EU;

3. enhancing the transparency of security properties of PDEs; and

4. enabling businesses and consumers to use PDEs securely, including through requirements for vulnerability and incident handling.

As an EU regulation, the CRA will be directly applicable in all EU Member States. For matters covered by the CRA, Member States should not impose additional cybersecurity requirements for making available PDEs on the EU market. However, Member States would be entitled to impose additional cybersecurity requirements for the procurement or use of PDEs for specific purposes (such as national security or defence), provided that such requirements are necessary and proportionate.

SCOPE OF APPLICATION

The CRA imposes obligations and requirements upon economic operators for the design, development and production of PDEs made available on the EU market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect, logical or physical, data connection to a device or network. This is an amendment to the scope proposed by the Commission, which applied only to PDEs whose "intended or reasonably foreseeable use" included connection to a device or network.

The "economic operators" in scope are manufacturers, authorised representatives, importers and distributors, and any other natural or legal person subject to obligations in relation to the manufacture of PDEs or making them available on the market (e.g., open-source software stewards), in each case where they supply a PDE for distribution or use in the EU in the course of a commercial activity.

Typical examples of PDEs include laptops, mobile devices, smart cards, routers, industrial control systems, mobile apps, video games and computer processing units. Remote data processing solutions are included where these are designed and developed by, or under the responsibility of, the manufacturer and the remote processing is necessary for the PDE to perform any of its functions.

The co-legislators clarified that, for example, cloud-enabled functionality provided by the manufacturer of smart home devices that enable users to control the device at a distance will fall within scope (e.g., connected home cameras). However, cloud services designed and developed outside the responsibility of a PDE manufacturer (e.g., IaaS service developed by a third-party cloud provider) are not within scope of the CRA.

The co-legislators also specified that the CRA does not apply to spare parts made available on the EU market that are manufactured according to the same specifications as the identical PDE components they are intended to replace.

The CRA excludes from its scope certain products and/or fields, mainly medical and in-vitro diagnostic devices, motor vehicles (which are addressed by other EU regulations), spare parts for PDEs as well as PDEs which are developed or modified exclusively for national security or defence purposes or specifically designed to process classified information.

The co-legislators made some clarifications to the notion of "commercial activity" in scope. This not only includes charging a price for a product, but also includes charging a price for technical support services (where this does not only recuperate costs), an intention to monetise (e.g., providing a software platform through which the manufacturer monetises other services), requiring as a condition for use the processing of personal data (for reasons other than improving the security, compatibility or interoperability of the software), and accepting donations in excess of costs with the intention of making a profit.

Overlap with EU AI Act

The co-legislators recognise that AI systems may be caught as PDEs under the CRA. The CRA therefore provides that PDEs that are also high-risk AI systems under the draft AI Act, which will be required under that Act to achieve an appropriate level of cybersecurity, will be deemed to comply with those requirements if the security requirements under the CRA are met

KEY OBLIGATIONS

The CRA imposes several obligations upon relevant economic operators, namely manufacturers, authorised representatives, importers and distributors, and any other natural or legal person subject to obligations in relation to the manufacture of PDEs or making them available on the market (e.g., open-source software stewards).

The key obligation imposed on relevant economic operators is that PDEs meet essential cybersecurity requirements set out in Annex I to the CRA. These requirements include ensuring that:

- PDEs do not have known exploitable vulnerabilities (i.e., vulnerabilities which have the potential to be effectively used by an adversary under practical operational conditions);
- any vulnerabilities (i.e., any weakness, susceptibility or flaw that can be exploited by a cyber threat) can be addressed through security updates and within an appropriate time frame;
- PDEs are protected against unauthorised data access, modification or manipulation, and that any data corruption or possible unauthorised access is reported;
- PDEs are designed, developed and produced to limit attack surfaces, to 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; and
- the principle of data minimisation is followed.

I. MANUFACTURERS

General obligations

- **Cybersecurity risk assessments:** First, manufacturers will be required to assess the cybersecurity risks associated with PDEs based on the intended purpose and reasonably foreseeable use of the PDE, as well as the conditions of use of the PDE. Manufacturers must take the cybersecurity risk assessment outcome into account during the planning, design, development, production, delivery and maintenance phases of the life cycle of PDEs (the so-called "*support period*"), with a view to minimising cybersecurity risks, preventing security incidents and minimising the impact of such incidents. Cybersecurity risk assessments – to be included in the technical documentation of PDEs placed on the market – must be appropriately documented, updated and comprise the analysis of risk associated with the intended purpose or foreseeable use of the PDE as well as the conditions of its use.

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

- **Conformity assessments:** Manufacturers will be required to conduct conformity assessments to establish whether essential cybersecurity requirements have been fulfilled in relation to the PDE and that the manufacturer meets the vulnerability handling requirements, except in limited cases where a presumption of conformity exists (e.g., PDEs which are in conformity with harmonised standards that are to be determined in due course by a standardisation organisation designated by the Commission).

The CRA sets out different obligations depending on the criticality of PDEs. 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 "important products" (subdivided into "Class I" and "Class II"), due to the cybersecurity 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, would include the involvement of an authorised third party even where the product complies with harmonised standards, common specifications or European cybersecurity certifications). Lastly, the category of "critical products" includes PDEs which carry a significant risk of adverse effects in terms of ability to disrupt, control or damage a large number of other PDEs through direct manipulation.

How are PDEs classified?

- **Examples of Class I** include identity management systems software and hardware (including authentication and access control readers), stand-alone and embedded browsers, password managers, software that searches for, removes, or quarantines malicious software, VPN, network interfaces, security information and event management systems, boot managers, network interfaces, public key infrastructure and digital certificate issuance software, operating systems, routers, firewalls, microcontrollers and microprocessors with security-related functionalities, smart home products with security-related functionalities and smart home general purpose virtual assistants, certain internet-connected toys, and certain personable wearable products.
- **Examples of Class II** include operating systems for servers, firewalls, intrusion detection or prevention systems, tamper-resistant microprocessors and microcontrollers.
- **Examples of "critical products"** include hardware devices with security boxes, smart meter gateways within smart metering systems, and smartcards or similar devices, including secure elements.

- **Declaration of conformity:** Once a manufacturer has complied with the conformity assessment requirement, it will be required to draw up an EU declaration of conformity with essential requirements prescribed by the CRA and, where applicable, of the other relevant EU legislation applicable to the PDE. A single EU declaration of conformity will be required for compliance with all relevant EU legislation and 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 must be provided with the PDE in the instructions to a user, along with an Internet address where the declaration can be accessed. Manufacturers must also keep the technical documentation and the EU declaration of conformity for at least 10 years after the PDE has been placed on the market and provide the relevant documents upon request of the market surveillance authorities (MSAs). Further, manufacturers must affix the "CE" marking on the PDEs (indicating that the manufacturer has checked that the product complies with EU requirements). By drawing up the EU declaration of conformity, the manufacturer assumes responsibility for the compliance of the product.

- **Vulnerability handling:** 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 will be required to ensure that product vulnerabilities are handled effectively. This includes:
  - identifying and documenting vulnerabilities;
  - applying effective regular testing and addressing and remediating vulnerabilities without delay;
  - providing security updates in a timely manner and security patches free of charge 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.

The co-legislators' amendments allow for a support period of less than five years where the lifetime of the PDE is less than five years and this shorter lifetime is justified by the nature of the product. In these cases, the manufacturer should ensure vulnerability handling for that lifetime. For example, subscription-based software or apps that become unavailable once the subscription expires may have a shorter lifetime where they can reasonably be expected to be in use for less than 5 years. Where the time the PDE is reasonably expected to be in use is longer than five years (e.g., hardware components such as motherboards or microprocessors, network devices such as routers, modems or switches, as well as software, such as operating systems), manufacturers should accordingly guarantee longer support times. It is the responsibility of the manufacturer to determine the relevant support period, taking into account relevant factors, including reasonable user expectations, the nature of the PDE, and relevant EU law determining the lifetime of such PDE.

Incident reporting

- **Informing authorities:** If a manufacturer becomes aware of any actively exploited vulnerability (defined as a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the owner) contained in the PDE, or of any severe incident having an impact on the security of the PDE (**severe incident**), it must report it and notify the Computer Security Incident Response Team (CSIRT) and the EU Agency for Cybersecurity (ENISA) without undue delay and in any event within 24 hours of becoming aware, by means of an early warning notification. A specific Member State CSIRT may be designated as the co-ordinator, where the manufacturer has its main establishment in the EU. Also, unless the relevant information has already been provided, the manufacturer shall submit a vulnerability or incident notification, without undue delay and in any event within 72 hours. The manufacturer shall also submit a final report no later than 14 days after a corrective or mitigating measure is available (in the case of an actively exploited vulnerability), or within one month after the submission of the incident notification (in the case of a severe incident). The information to be provided at each stage differs according to whether an actively exploited vulnerability or severe incident is being reported.

As well as creating this distinction between the types of cybersecurity incidents that require reporting, the co-legislators have clarified that the act of notifying an incident or actively exploited vulnerability will not subject the notifying natural or legal person to increased liability. The co-legislators also require ENISA to establish, manage and maintain a 'single reporting platform' for notifications.

- **Informing users**: The manufacturer must also inform the impacted users of the PDE (and, where appropriate, all users) in a timely manner about an actively exploited vulnerability or a severe incident and, where necessary, about risk mitigation and any corrective measures that they might deploy to mitigate the impact.
- **Informing the public**: In addition, if informing the wider public is needed to prevent or mitigate a severe incident that affects the security of PDE, to handle an ongoing incident, or if revealing the incident is in the public interest, the CSIRT designated as coordinator may, after consulting with the manufacturer (and where appropriate with the ENISA's involvement), inform the public about the incident or require that the manufacturer do so.

Technical documentation and transparency

Manufacturers will be required to draw up technical documentation, which must contain all relevant data used by the manufacturer to ensure that the PDE and the processes put in place by the manufacturer comply with the essential cybersecurity requirements under 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, the software bill of materials (if applicable), a copy of the EU declaration of conformity, and the additional information required by any relevant EU acts (such as other product regulations).

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

The co-legislators added more detail to the requirements for manufacturers to provide certain information in an easily accessible manner, such as their contact details, their designated 'single point of contact' and the end date of the PDE's support period. For example, the end date of the support period must, where applicable, be on the PDE, its packaging or be provided by digital means at the time of purchase.

Appointed representatives

Manufacturers may appoint authorised representatives by a written mandate to perform specific tasks required by the CRA. Authorised representatives can take on some tasks under the CRA (e.g., in relation to co-operation with market surveillance authorities) but not certain obligations (e.g., responsibility for the cybersecurity risk assessment).

II. 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 must 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, and that the PDE is accompanied by the required information, documentation and instructions.

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

Importers and distributors will also be subject to certain other reporting obligations (e.g., informing, without undue delay, the manufacturer and the market surveillance authorities where PDEs present a significant cybersecurity risk), product recall, withdrawal or corrective measures where PDEs not in conformity with the CRA are made available on the market, and record-keeping requirements (e.g., keeping a copy of the EU declaration of conformity and all documentation necessary to demonstrate the conformity of the PDEs and processes put in place by manufacturers with the CRA at the disposal of the market surveillance authorities, in a language which can be easily understood by such authorities).

III. OPEN-SOURCE SOFTWARE STEWARDS

The co-legislators added a focus on free and open-source software in the CRA, including the concept of an 'open-source software steward' upon whom the CRA imposes specific obligations. A steward is any legal person, other than a manufacturer, which has the purpose or objective of systematically providing support on a sustained basis for the development of specific PDEs qualifying as free and open-source software that are intended for commercial activities, and ensures the viability of those products.

A steward must put in place and document in a verifiable manner a cybersecurity policy which fosters the development of secure PDEs and demonstrates effective handling of vulnerabilities by the developers of PDEs. The cybersecurity policy must take into account the specific nature of the open-source software steward and the legal and organisational arrangements it is subject to.

Open-source software stewards must co-operate with the market surveillance authorities and provide them with the relevant documentation at their request, with a view to mitigating the cybersecurity risks posed by a PDE qualifying as free and open-source software.

MARKET SURVEILLANCE, ENFORCEMENT AND PENALTIES

Guidance

In order to ease implementation and ensure consistency, the Commission will publish guidelines to assist economic operators with applying the provisions of the CRA, with a particular focus on how to facilitate compliance by microenterprises, small enterprises and medium-sized enterprises.

Enforcement

Member States	EU level
Member States will each designate one or several "market surveillance authorities" (**MSAs**) 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. Economic operators should fully co-operate with market surveillance authorities and other competent authorities.	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 representatives of the designated MSAs and, if appropriate, representatives of single liaison offices. 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 with respect to the design, development and vulnerability handling of such products)[1].	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 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, or where the Commission considers the measure implemented to be contrary to EU law.

1 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.

Penalties and Sanctions

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

- Breaches of the essential cybersecurity requirements, conformity assessment and reporting obligations may result in administrative fines of up to EUR 15 million or up to 2.5% of annual global turnover, whichever is higher.
- Breaches of the other CRA rules, including requirements to appoint an authorised representative, obligations applicable to importers or distributors, and certain requirements for the EU declaration of conformity, technical documentation and CE marking, may result in administrative fines of up to EUR 10 million or up to 2% of annual global turnover, whichever is higher.
- Organisations which provide incorrect, incomplete or misleading information face administrative fines of up to EUR 5 million or, if the offender is an undertaking, up to 1% of annual turnover.

Size and market share of an operator are among the factors to be taken into account when determining the amount of an administrative fine.

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

NEXT STEPS AND TRANSITIONAL PROVISIONS

The CRA is now subject to formal approval by the Council. Following its adoption, the CRA will be enacted on the 20th day after its publication in the Official Journal, which means that the CRA is expected to be finalised in the second quarter of 2024. Various transition periods will apply, with the CRA expected to be fully applicable from 2027.

Once in force, the relevant economic operators will be given a grace period of up to 36 months to adjust to the provisions of the CRA, during which time further regulatory guidance is expected. There is a shorter, 21-month, grace period for reporting obligations concerning actively exploited vulnerabilities and severe incidents, and an 18-month grace period regarding the provisions on notification of conformity assessment bodies.

There is a 42-month transition window from the CRA's entry into force, during which the EU type-examination certificates and approval decisions on cybersecurity shall remain valid, unless they expire before that date, or unless specified in any other EU Act. PDEs that have been placed on the market prior to the expiry of the CRA's 36 month grace period will not be subject to the requirements of the CRA, unless they undergo substantial modifications. If a new category of PDE is added to Annex III (Important PDEs) and is moved from Class I to Class II, in most cases there will be a transition period of 12 months before the relevant conformity assessment procedures apply.

It will be crucial for affected businesses to begin preparing for compliance, including integrating CRA security requirements into the design cycle of their products and creating or amending internal procedures to meet CRA rules.

AUTHORS AND CONTRIBUTORS

Dessislava Savova
Partner, Head of the Continental Europe Tech Group
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

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

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

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

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

Alexander Kennedy
Knowledge Director – CE Tech Group
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Rita Flakoll
Global Head of Tech Group Knowledge
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

Maria Giulia Tammaro and Leonardo Panerai contributed to the drafting of this briefing

CLIFFORD

CHANCE

www.cliffordchance.com

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

2403-010255