SZECSKAY
ATTORNEYS AT LAW

April 2026

Overview of the main obligations and sanctions under the EU's Cyber Resilience Act

Under the EU's Cyber Resilience Act (Regulation 2024/2847, hereinafter referred to as "**CRA**"), the organisations concerned (manufacturers, importers, distributors of products with digital elements as well as so-called economic operators) are required to fulfill certain obligations. The CRA is already effective and will become applicable gradually (see below).

For the purposes of the CRA,

'*product with digital elements*' means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

'*manufacturer*' means a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge;

'*importer*' means a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union; ('placing on the market' means the first making available of a product with digital elements on the Union market and 'making available on the market' means the supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge);

'*distributor*' means a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties;

'*economic operator*' means the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations in relation to the manufacture of products with digital elements or to the making available of products with digital elements on the market in accordance with the CRA.

The CRA is already effective and will be applicable as from 11 December 2027, except for provisions on the reporting obligations of manufacturers which will be applicable as of 11 September 2026 and Chapter IV governing the notification of conformity assessment bodies, which provisions will be applicable from 11 June 2026.

Though the deadline of 11 December 2027 may seem distant, it is worth noting that complying with the obligations takes time; therefore, it is advisable to begin preparations

and take the necessary steps and measures as soon as possible.

Further, products with digital elements that have been placed on the market before 11 December 2027 are subject to the requirements set out in the CRA only if, from that date, those products are subject to a substantial modification. However, **the obligations laid down in Article 14 (*i.e.* reporting obligations of manufacturers) apply to all products with digital elements that fall within the scope of the CRA that have been placed on the market before 11 December 2027**.

It is worth noting that even an importer or distributor is considered to be a manufacturer for the purposes of the CRA and is subject to the manufacturer's obligations (including those laid down in Article 14), where that importer or distributor places a product with digital elements on the market under its name or trademark or carries out a substantial modification of a product with digital elements already placed on the market (Article 21). Further, a natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of a product with digital elements and makes that product available on the market, is considered to be a manufacturer for the purposes of the CRA and is subject to the manufacturer's obligations (for the part of the product with digital elements that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product) (Article 22).

In case of non-compliance, the amount of fine can be very high. Depending on the type of non-compliance, the amount of fine can be up to EUR 15 million or, if the offender is an undertaking, up to 2,5% of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

It is worth noting that in light of the CRA, Hungarian legislation may also be enacted that could similarly impose certain obligations.

Under the CRA, the organisations concerned can expect to fulfill the following main obligations.

Overview

Who does the CRA apply to (and who does it not apply to)?

The CRA applies to products with digital elements made available on the 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.

The CRA applies to

(i) rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products,

(ii) essential cybersecurity requirements for the design, development and production of products with digital elements, and obligations for economic operators (including manufacturers, importers, distributors) in relation to those products with respect to

cybersecurity,

(iii) vulnerability management procedures implemented by manufacturers during the expected lifetime of products with digital elements and obligations for economic operators in relation to those processes, and

(iv) market surveillance.

The CRA does not apply to

- products with digital elements that fall within the scope of Regulation (EU) 2017/745 on medical devices,
- products with digital elements falling within the scope of Regulation (EU) 2017/746 on in vitro diagnostic medical devices,
- products containing digital elements that fall within the scope of Regulation (EU) 2019/2144 on the type approval requirements for motor vehicles and their trailers, and for systems, components, and separate technical units intended for such vehicles, with regard to general safety and the protection of vehicle occupants and vulnerable road users,
- products with digital elements certified under Regulation (EU) 2018/1139 on common rules in the field of civil aviation,
- maritime equipment falling within the scope of Regulation (EU) 2014/90,
- spare parts marketed for the purpose of replacing identical components of products with digital elements and manufactured in accordance with the same specifications as the components they are intended to replace,
- products with digital elements that have been developed or modified exclusively for national security or defence purposes, as well as products specifically designed for the processing of classified data.

Products with digital elements **may be placed on the market only if**

(a) **they comply with the essential cybersecurity requirements set out in Part I of Annex I of the CRA**, provided that they are properly installed, maintained, and used in accordance with their intended purpose or under reasonably foreseeable conditions, and, where applicable, the necessary security updates have been installed; and

(b) the **procedures implemented by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I of the CRA**.

1 Obligations of the manufacturers

Article 13 (Obligations of manufacturers)

(i) When placing a product with digital elements on the market, manufacturers must ensure that it has been **designed, developed and produced in accordance with the essential cybersecurity requirements** set out in Part I of Annex I of the CRA.

(ii) Manufacturers must undertake an **assessment of the cybersecurity risks** associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of

the product with digital elements.

(iii) **Documenting and updating the cybersecurity risk assessment** during the support period. (Manufacturers must define the support period to reflect the length of time during which the product is expected to be used.)

(iv) **Factors to be considered during the cybersecurity risk assessment** (see Article 13 (3) of the CRA). For example, the assessment must indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I of the CRA are applicable to the relevant product with digital elements and how those requirements are implemented. It must also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I of the CRA.

(v) **Inclusion of the risk assessment into the technical documentation**.

(vi) **Due diligence must be exercised** when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product with digital elements.

(vii) Upon identifying a vulnerability in a component, which is integrated in the product with digital elements, **reporting of the vulnerability to the entity manufacturing** or maintaining **the component**, and **addressing** and remediation of **the vulnerability** in accordance with the vulnerability handling requirements set out in Part II of Annex I of the CRA.

(viii) **Systematic documentation**, in a manner that is proportionate to the nature and the cybersecurity risks, **of the relevant cybersecurity aspects** concerning the products with digital elements. Where applicable, **update of the cybersecurity risk assessment** of the products.

(ix) When placing a product with digital elements on the market, and for the support period, ensuring that **vulnerabilities** of that product, including its components, **are handled effectively** and in accordance with the essential cybersecurity requirements.

(x) Having **appropriate policies** and procedures, including coordinated vulnerability disclosure policies.

(xi) Ensuring that each **security update** which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer.

(xii) **Preparation of technical documentation** (Article 31) prior to placing a product with digital elements on the market.

(xiii) **Conduct of** the selected **conformity assessment procedure** (Article 32).

(xiv) **Preparation of an EU declaration of conformity** (Article 28) and **affixing the CE marking** to the product (Article 30).

(xv) The **technical documentation and the EU declaration of conformity must be made available** to market surveillance authorities for at least 10 years after the product is placed on the market or until the end of the warranty period, whichever is longer.

(xvi) Ensuring that the manufacturer's **products with digital elements bear a type, batch or serial number** or other element allowing their identification, or, where that is not possible, that that information is provided on their packaging or in a document accompanying the product with digital elements.

(xvii) Manufacturers must **indicate the name, registered trade name or registered trademark of the manufacturer**, and the postal address, email address or other digital contact details, as well as, where applicable, the website where the manufacturer can be contacted, on the product with digital elements, on its packaging or in a document accompanying the product with digital elements.

(xviii) **Designation of a single point of contact** to enable users to communicate directly and rapidly with them.

(xix) Ensuring that **products with digital elements are accompanied by the information and instructions to the user** set out in Annex II, in paper or electronic form.

(xx) Ensuring that the **end date of the support period (at least the month and the year) is clearly specified** at the time of purchase in an easily accessible manner and, where applicable, on the product with digital elements, its packaging or by digital means.

(xxi) Provision of a copy of the **EU declaration of conformity or a simplified EU declaration of conformity** with the product with digital elements.

(xxii) If the manufacturer knows or has reason to believe that a product with digital elements or the procedures implemented by the manufacturer do not comply with the essential cybersecurity requirements, the necessary **corrective measures must be taken** (correction, recall, withdrawal from the market).

(xxiii) **Cooperation with authorities**, provision of documents.

(xxiv) **Notification** to the authorities and users regarding the cessation of operations.

Article 14 (Reporting obligations of manufacturers)

(i) **Early warning notification** of an actively exploited vulnerability: notification to the CSIRT and ENISA within 24 hours of becoming aware of it, and

(ii) **Vulnerability notification** regarding an actively exploited vulnerability within 72 hours of becoming aware of it, including certain information, and

(iii) **Final report** no later than 14 days after a corrective or mitigating measure becomes available, providing certain information.

(iv) **Notification of any severe incident** having an impact on the security of the product

with digital elements that the manufacturer becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA.

(v) **Notification of a severe incident** within 24 hours of becoming aware of it, including certain information, and

(vi) **Notification of an incident** within 72 hours of becoming aware of it, including certain information, and

(vii) **Final notification** no later than one month after the notification referred to in point (vi) above, including certain information.

(viii) The CRA specifies when an incident is deemed a severe incident and names the Member State in which the notification must be filed.

(viii) **Notification of users** of both actively exploited vulnerabilities and severe incidents.

2 Obligations of importers (Article 19)

(i) Importers may place on the market only products with digital elements that **comply with the essential cybersecurity requirements set out in Part I of Annex I of the CRA** and where the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I of the CRA.

(ii) Ensuring that

a) the manufacturer has duly carried out the **appropriate conformity assessment procedures**,
b) the manufacturer has drawn up the **technical documentation**,
c) the **CE marking** is affixed to the product with digital element, and is accompanied by the **EU declaration of conformity and the user information and instructions for use**, and
d) the manufacturer has complied with the requirements concerning **marking, the manufacturer's details and contact information and the end date of the support period**.

(iii) Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the CRA, the importer **may not place the product on the market** until that product or the processes put in place by the manufacturer have been brought into conformity with the CRA. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer must inform the manufacturer and the market surveillance authorities to that effect.

(iv) Where an importer has reason to believe that a product with digital elements may present a significant cybersecurity risk in light of non-technical risk factors, the importer **must inform the market surveillance authorities** to that effect.

(v) Importers must **indicate their name, registered trade name or registered**

trademark, the postal address, email address or other digital contact as well as, where applicable, **the website** at which they can be contacted on the product with digital elements or on its packaging or in a document accompanying the product with digital elements.

(vi) Importers who know or have reason to believe that a product with digital elements which they have placed on the market is not in conformity with the CRA **must immediately take the corrective measures** necessary to ensure that the product with digital elements is brought into conformity with the CRA, or to withdraw or recall the product, if appropriate.

(vii) Upon becoming aware of a vulnerability in the product with digital elements, importers **must inform the manufacturer without undue delay about that vulnerability**. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers **must immediately inform the market surveillance authorities** of the Member States in which they have made the product with digital elements available on the market to that effect.

(viii) Importers must, for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, **keep a copy of the EU declaration of conformity** at the disposal of the market surveillance authorities and ensure that the **technical documentation can be made available** to those authorities, upon request.

(ix) **Cooperation with authorities** (provision of information and documentation, elimination of cybersecurity risks).

(x) Where the importer of a product with digital elements becomes aware that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in the CRA, the importer **must inform the relevant market surveillance authorities** about this situation, **as well as**, by any means available and to the extent possible, **the users** of the products with digital elements placed on the market.

3 Obligations of importers (Article 20)

(i) Before making a product with digital elements available on the market, distributors **must verify that**

(a) the product with digital elements bears the **CE marking**,
(b) the **manufacturer and the importer have complied with certain obligations** (Article 13(15), (16), (18), (19) and (20) and Article 19(4)), **and have provided all necessary documents to the distributor**.

(ii) Where a distributor considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I of the CRA, the distributor **must not make the product with digital elements available on the market** until that product or the processes put in place by the manufacturer have been brought into conformity with the CRA. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor **must inform**, without undue delay, **the manufacturer**

and the market surveillance authorities to that effect.

(iii) Distributors who know or have reason to believe, on the basis of information in their possession, that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the CRA **must make sure that the corrective measures** necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity, or to withdraw or recall the product, if appropriate, **are taken**.

(iv) Upon becoming aware of a vulnerability in the product with digital elements, distributors **must inform the manufacturer without undue delay about that vulnerability**. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors **must immediately inform the market surveillance authorities** of the Member States in which they have made the product with digital elements available on the market to that effect.

(v) **Cooperation with authorities** (provision of information and documentation, elimination of cybersecurity risks).

(vi) Where the distributor of a product with digital elements becomes aware that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in the CRA, the distributor **must inform**, without undue delay, **the relevant market surveillance authorities** about this situation, **as well as**, by any means available and to the extent possible, **the users** of the products with digital elements placed on the market.

4 Identification of economic operators (Article 23)

(i) Economic operators **must**, on request, **provide the market surveillance authorities** with the following information:
(a) the **name and address of any economic operator who has supplied them** with a product with digital elements,
(b) where available, the **name and address of any economic operator to whom they have supplied** a product with digital elements.

(ii) Economic operators **must be able to present the information** referred to in clause (i) above **for 10 years** after they have been supplied with the product with digital elements and for 10 years after they have supplied the product with digital elements.

5 Other provisions

The CRA also contains rules on the conformity of products with digital elements, the notification of conformity assessment bodies and market surveillance and enforcement.

6 Conclusions

First, it is important to ascertain if the given entity is covered by the CRA. If the answer is in the affirmative, the status of the entity has to be determined followed by the identification of obligations and the corresponding deadline until which compliance is to take place.

This summary has been prepared by the data protection and cyber security team in our office. The contents of this document do not qualify as legal advice. Specific legal advice should be sought for specific matters.

Dr. KOVÁCS ZOLTÁN BALÁZS, LL.M.
zoltan.kovacs@szecskay.com

Dr. ÁDÁM BENEDEK
benedek.adam@szecskay.com