EU Cyber Resilience Act – 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 Cyber Resilience Act

Issued 9/15/2022

Addresses:

- a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;
- (b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;
- (c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;
- (d) rules on market surveillance and enforcement of the above-mentioned rules and requirements

EU Cyber Resilience Act

Scope:

- Applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network
  - Does not apply to some products that meet some specific EU regulations
- The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential requirements set out in Annex I may be limited or excluded, where:
  - (a) such limitation or exclusion is consistent with the overall regulatory framework applying to those products; and
  - (b) the sectoral rules achieve the same level of protection as the one provided for by this Regulation
- The Commission is empowered to adopt delegated acts in accordance with Article 50 to amend this Regulation specifying whether such limitation or exclusion is necessary, the concerned products and rules, as well as the scope of the limitation, if relevant.
- Does not apply to products with digital elements developed exclusively for national security or military purposes or to products specifically designed to process classified information

EU Cyber Resilience Act

Key Definitions:

- ‘product with digital elements’: any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately
- ‘critical product with digital elements’: a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III
- ‘highly critical product with digital elements’: a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(5)
- ‘software’: the part of an electronic information system which consists of computer code
- ‘hardware’: a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data
- ‘significant cybersecurity risk’: a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption

EU Cyber Resilience Act

Requirements for products with digital elements:

- they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated, and
- the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I

Critical products with digital elements**:**

- Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products
- Subject to the conformity assessment procedures referred to in Article 24(2) and (3)

EU Cyber Resilience Act

Factors to determine level of cybersecurity risk:

- (a) the cybersecurity-related functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:
  - (i) it is designed to run with elevated privilege or manage privileges;
  - (ii) it has direct or privileged access to networking or computing resources;
  - (iii) it is designed to control access to data or operational technology;
  - (iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection
- (b) the intended use in sensitive environments, including in industrial settings;
- (c) the intended use of performing critical or sensitive functions, such as processing of personal data;
- (d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;
- (e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact

EU Cyber Resilience Act

Essential Cybersecurity Requirements (Annex I):

- (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;
- (2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;
- (3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:
  - (a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;
  - (b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;
  - (c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;
  - (d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

EU Cyber Resilience Act

Essential Cybersecurity Requirements (Annex I) (cont):

- (3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:
  - (e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product (‘minimisation of data’);
  - (f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;
  - (g) minimise their own negative impact on the availability of services provided by other devices or networks;
  - (h) be designed, developed and produced to limit attack surfaces, including external interfaces;
  - (i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
  - (j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;
  - (k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users

EU Cyber Resilience Act

Vulnerability Handling Requirements (Annex I):

Manufacturers of the products with digital elements shall:

- (1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;
- (2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;
- (3) apply effective and regular tests and reviews of the security of the product with digital elements;
- (4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;
- (5) put in place and enforce a policy on coordinated vulnerability disclosure;

EU Cyber Resilience Act

Vulnerability Handling Requirements (Annex I) (cont):

Manufacturers of the products with digital elements shall:

- (6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;
- (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;
- (8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken

EU Cyber Resilience Act

Critical Products with Digital Elements (Annex III):

Class I:

- Identity management systems software and privileged access management software;
- Standalone and embedded browsers;
- Password managers;
- Software that searches for, removes, or quarantines malicious software;
- Products with digital elements with the function of virtual private network (VPN);
- Network management systems;
- Network configuration management tools;
- Network traffic monitoring systems;
- Management of network resources;
- Security information and event management (SIEM) systems;
- Update/patch management, including boot managers;
- Application configuration management systems;
- Remote access/sharing software;
- Mobile device management software;

EU Cyber Resilience Act

Critical Products with Digital Elements (Annex III):

Class I:

- Physical network interfaces;
- Operating systems not covered by class II;
- Firewalls, intrusion detection and/or prevention systems not covered by class II;
- Routers, modems intended for the connection to the internet, and switches, not covered by class II;
- Microprocessors not covered by class II;
- Microcontrollers;
- Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
- Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
- Industrial Internet of Things not covered by class II

EU Cyber Resilience Act

Critical Products with Digital Elements (Annex III):

Class II:

- Operating systems for servers, desktops, and mobile devices;
- Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
- Public key infrastructure and digital certificate issuers;
- Firewalls, intrusion detection and/or prevention systems intended for industrial use;
- General purpose microprocessors;
- Microprocessors intended for integration in programmable logic controllers and secure elements;
- Routers, modems intended for the connection to the internet, and switches, intended for industrial use;
- Secure elements;

EU Cyber Resilience Act

Critical Products with Digital Elements (Annex III):

Class II:

- Hardware Security Modules (HSMs);
- Secure cryptoprocessors;
- Smartcards, smartcard readers and tokens;
- Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
- Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
- Robot sensing and actuator components and robot controllers;
- Smart meters

EU Cyber Resilience Act

Conformity Assessment (Article 24):

- Manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements by using one of the following procedures:
  - (a) the internal control procedure (based on module A) set out in Annex VI; or
  - (b) the EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or
  - (c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI

EU Cyber Resilience Act

Conformity Assessment (Article 24):

- Where, in assessing the compliance of the critical product with digital elements of class I as set out in Annex III and the processes put in place by its manufacturer with the essential requirements set out in Annex I, the manufacturer or the manufacturer's authorised representative has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes as referred to in Article 18, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential requirements to either of the following procedures:
  - (a) EU-type examination procedure (based on module B) provided for in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or
  - (b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI

EU Cyber Resilience Act

Conformity Assessment (Article 24):

- Where the product is a critical product with digital elements of class II as set out in Annex III, the manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements set out in Annex I by using one of the following procedures:
  - (a) EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or
  - (b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI
- Manufacturers of products with digital elements that are classified as EHR systems under the scope of Regulation [the European Health Data Space Regulation] shall demonstrate conformity with the essential requirements laid down in Annex I of this Regulation using the relevant conformity assessment procedure as required by Regulation [Chapter III of the European Health Data Space Regulation]
- Notified bodies shall take into account the specific interests and needs of small and medium sized enterprises (SMEs) when setting the fees for conformity assessment procedures and reduce those fees proportionately to their specific interests and needs

EU Cyber Resilience Act

CONFORMITY ASSESSMENT PROCEDURE BASED ON INTERNAL CONTROL (Artificial Intelligence Act Annex VI):

- The conformity assessment procedure based on internal control is the conformity assessment procedure based on points 2 to 4
- The provider verifies that the established quality management system is in compliance with the requirements of Article 17
- The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in Title III, Chapter 2
- The provider also verifies that the design and development process of the AI system and its post-market monitoring as referred to in Article 61 is consistent with the technical documentation

EU Cyber Resilience Act

Hi-Risk AI Systems (Article 8):

- Products with digital elements classified as high-risk AI systems in accordance with Article [Article 6] of Regulation [the AI Regulation] which fall within the scope of this Regulation, and fulfil the essential requirements set out in Section 1 of Annex I of this Regulation, and where the processes put in place by the manufacturer are compliant with the essential requirements set out in Section 2 of Annex I, shall be deemed in compliance with the requirements related to cybersecurity set out in Article [Article 15] of Regulation [the AI Regulation], without prejudice to the other requirements related to accuracy and robustness included in the aforementioned Article, and in so far as the achievement of the level of protection required by those requirements is demonstrated by the EU declaration of conformity issued under this Regulation
- For the products and cybersecurity requirements referred to in paragraph 1, the relevant conformity assessment procedure as required by Article [Article 43] of Regulation [AI Regulation] shall apply. For the purpose of that assessment, notified bodies which are entitled to control the conformity of the high-risk AI systems under the Regulation [AI Regulation] shall be also entitled to control the conformity of the high-risk AI systems within the scope of this Regulation with the requirements set out in Annex I to this Regulation, provided that the compliance of those notified bodies with the requirements laid down in Article 29 of this Regulation have been assessed in the context of the notification procedure under Regulation [AI Regulation]

EU Cyber Resilience Act

Hi-Risk AI Systems (Article 8):

- By derogation from paragraph 2, critical products with digital elements listed in Annex III of this Regulation, which have to apply the conformity assessment procedures referred to in Articles 24(2)(a), 24(2)(b), 24(3)(a) and 24(3)(b) under this Regulation and which are also classified as high-risk AI systems according to Article [Article 6] of the Regulation [AI Regulation] and to which the conformity assessment procedure based on internal control referred to in Annex [Annex VI] to Regulation [the AI Regulation] applies, shall be subject to the conformity assessment procedures as required by this Regulation in so far as the essential requirements of this Regulation are concerned

EU Cyber Resilience Act

Technical documentation (Article 23):

- Technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential requirements set out in Annex I. It shall at least contain the elements set out in Annex V
- Technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, during the expected product lifetime or during a period of five years after the placing on the market of a product with digital elements, whichever is shorter
- For products with digital elements referred to in Articles 8 (High Risk AI Sytems) and 24(4) that are also subject to other Union acts, one single technical documentation shall be drawn up containing the information referred to in Annex V of this Regulation and the information required by those respective Union acts
- Technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body

BACKUP

EU Cyber Resilience Act Chapters and Annexes

Chapter I, General provisions.

- Article 1, Subject matter, Cyber Resilience Act, 15.9.2022
- Article 2, Scope, Cyber Resilience Act, 15.9.2022
- Article 3, Definitions, Cyber Resilience Act, 15.9.2022
- Article 4, Free movement, Cyber Resilience Act, 15.9.2022
- Article 5, Requirements for products with digital elements, Cyber Resilience Act, 15.9.2022
- Article 6, Critical products with digital elements, Cyber Resilience Act, 15.9.2022
- Article 7, General product safety, Cyber Resilience Act, 15.9.2022
- Article 8, High-risk AI systems, Cyber Resilience Act, 15.9.2022
- Article 9, Machinery products, Cyber Resilience Act, 15.9.2022

EU Cyber Resilience Act Chapters and Annexes

CHAPTER II - OBLIGATIONS OF ECONOMIC OPERATORS

- Article 10, Obligations of manufacturers, Cyber Resilience Act, 15.9.2022
- Article 11, Reporting obligations of manufacturers, Cyber Resilience Act, 15.9.2022
- Article 12, Authorised representatives, Cyber Resilience Act, 15.9.2022
- Article 13, Obligations of importers, Cyber Resilience Act, 15.9.2022
- Article 14, Obligations of distributors, Cyber Resilience Act, 15.9.2022
- Article 15, Cases in which obligations of manufacturers apply to importers and distributors, Cyber Resilience Act, 15.9.2022
- Article 16, Other cases in which obligations of manufacturers apply, Cyber Resilience Act, 15.9.2022
- Article 17, Identification of economic operators, Cyber Resilience Act, 15.9.2022

EU Cyber Resilience Act Chapters and Annexes

CHAPTER III - Conformity of the product with digital elements

- Article 18, Presumption of conformity, Cyber Resilience Act, 15.9.2022
- Article 19, Common specifications, Cyber Resilience Act, 15.9.2022
- Article 20, EU declaration of conformity, Cyber Resilience Act, 15.9.2022
- Article 21, General principles of the CE marking, Cyber Resilience Act, 15.9.2022
- Article 22, Rules and conditions for affixing the CE marking, Cyber Resilience Act, 15.9.2022
- Article 23, Technical documentation, Cyber Resilience Act, 15.9.2022
- Article 24, Conformity assessment procedures for products with digital elements, Cyber Resilience Act, 15.9.2022

EU Cyber Resilience Act Chapters and Annexes

CHAPTER IV - NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

- Article 25, Notification, Cyber Resilience Act, 15.9.2022
- Article 26, Notifying authorities, Cyber Resilience Act, 15.9.2022
- Article 27, Requirements relating to notifying authorities, Cyber Resilience Act, 15.9.2022
- Article 28, Information obligation on notifying authorities, Cyber Resilience Act, 15.9.2022
- Article 29, Requirements relating to notified bodies, Cyber Resilience Act, 15.9.2022
- Article 30, Presumption of conformity of notified bodies, Cyber Resilience Act, 15.9.2022
- Article 31, Subsidiaries of and subcontracting by notified bodies, Cyber Resilience Act, 15.9.2022
- Article 32, Application for notification, Cyber Resilience Act, 15.9.2022
- Article 33, Notification procedure, Cyber Resilience Act, 15.9.2022
- Article 34, Identification numbers and lists of notified bodies, Cyber Resilience Act, 15.9.2022

EU Cyber Resilience Act Chapters and Annexes

CHAPTER IV - NOTIFICATION OF CONFORMITY ASSESSMENT BODIES

- Article 35, Changes to notifications, Cyber Resilience Act, 15.9.2022
- Article 36, Challenge of the competence of notified bodies, Cyber Resilience Act, 15.9.2022
- Article 37, Operational obligations of notified bodies, Cyber Resilience Act, 15.9.2022
- Article 38, Information obligation on notified bodies, Cyber Resilience Act, 15.9.2022
- Article 39, Exchange of experience, Cyber Resilience Act, 15.9.2022
- Article 40, Coordination of notified bodies, Cyber Resilience Act, 15.9.2022

EU Cyber Resilience Act Chapters and Annexes

CHAPTER V - MARKET SURVEILLANCE AND ENFORCEMENT

- Article 41, Market surveillance and control of products with digital elements in the Union market, Cyber Resilience Act, 15.9.2022
- Article 42, Access to data and documentation, Cyber Resilience Act, 15.9.2022
- Article 43, Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk, Cyber Resilience Act, 15.9.2022
- Article 44, Union safeguard procedure, Cyber Resilience Act, 15.9.2022
- Article 45, Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk, Cyber Resilience Act, 15.9.2022
- Article 46, Compliant products with digital elements which present a significant cybersecurity risk, Cyber Resilience Act, 15.9.2022
- Article 47, Formal non-compliance, Cyber Resilience Act, 15.9.2022
- Article 48, Joint activities of market surveillance authorities, Cyber Resilience Act, 15.9.2022
- Article 49, Sweeps, Cyber Resilience Act, 15.9.2022

EU Cyber Resilience Act Chapters and Annexes

CHAPTER VI - DELEGATED POWERS AND COMMITTEE PROCEDURE

- Article 50, Exercise of the delegation, Cyber Resilience Act, 15.9.2022
- Article 51, Committee procedure, Cyber Resilience Act, 15.9.2022

CHAPTER VII - CONFIDENTIALITY AND PENALTIES

- Article 52, Confidentiality, Cyber Resilience Act, 15.9.2022
- Article 53, Penalties, Cyber Resilience Act, 15.9.2022

CHAPTER VIII - TRANSITIONAL AND FINAL PROVISIONS

- Article 54, Amendment to Regulation (EU) 2019/1020, Cyber Resilience Act, 15.9.2022
- Article 55, Transitional provisions, Cyber Resilience Act, 15.9.2022
- Article 56, Evaluation and review, Cyber Resilience Act, 15.9.2022
- Article 57, Entry into force and application, Cyber Resilience Act, 15.9.2022

EU Cyber Resilience Act Chapters and Annexes

- Annex 1, Cyber Resilience Act, 15.9.2022 - ESSENTIAL CYBERSECURITY REQUIREMENT
- Annex 2, Cyber Resilience Act, 15.9.2022 - INFORMATION AND INSTRUCTIONS TO THE USER
- Annex 3, Cyber Resilience Act, 15.9.2022 - CRITICAL PRODUCTS WITH DIGITAL ELEMENTS
- Annex 4, Cyber Resilience Act, 15.9.2022 - EU DECLARATION OF CONFORMITY
- Annex 5, Cyber Resilience Act, 15.9.2022 - CONTENTS OF THE TECHNICAL DOCUMENTATION