EU Cybersecurity Act –

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

EU Cybersecurity Act

Issued 7/6/2019

Addresses:

- Objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and
- A framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union

Proposed 2023 Amendment

EU Cybersecurity Act
Slight Change in Scope

From: a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union

To: a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, and managed security services in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

EU Cybersecurity Act New/Updated Key Definitions

- **European cybersecurity certification scheme**: A comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services, ICT processes, or managed security services
- **national cybersecurity certification scheme**: A comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services, ICT processes and managed security services falling under the scope of the specific scheme
- **European cybersecurity certificate**: A document issued by a relevant body, attesting that a given ICT product, ICT service, ICT process or managed security service has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme
- **managed security service**: A service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy
- **technical specifications**: A document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service, ICT process or managed security service

EU Cybersecurity Act New/Updated Key Definitions

- **assurance level**: A basis for confidence that an ICT product, ICT service, ICT process or managed security service meets the security requirements of a specific European cybersecurity certification scheme, and indicates the level at which an ICT product, ICT service, ICT process or managed security service has been evaluated but as such does not measure the security of the ICT product, ICT service, ICT process or managed security service concerned

- **conformity self-assessment**: An action carried out by a manufacturer or provider of ICT products, ICT services, ~~or~~ ICT processes or managed security services, which evaluates whether those ICT products, ICT services, ICT processes or managed security services meet the requirements of a specific European cybersecurity certification scheme

ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY)

EU Cybersecurity Act
ENISA Objectives

- Be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks
- Assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity
- Support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity
- Promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity

EU Cybersecurity Act
ENISA Objectives

- Contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents
- Promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market
- Contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services, ICT processes, and managed security services, thereby strengthening trust in the digital internal market and its competitiveness
- Promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses

EU Cybersecurity Act
ENISA Tasks - Market, cybersecurity certification, and standardisation - Changes

- Support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes and managed security services by*:*
  - monitoring developments, on an ongoing basis, in related areas of standardisation and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes;
  - preparing candidate European cybersecurity certification schemes (‘candidate schemes’) for ICT products, ICT services, ICT processes and managed security services;
  - evaluating adopted European cybersecurity certification schemes;
  - participating in peer reviews;
  - assisting the Commission in providing the secretariat of the ECCG
- Provide the secretariat of the Stakeholder Cybersecurity Certification Group
- Compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way
- Facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services, ICT processes and managed security services

Cybersecurity Certification Framework

EU Cybersecurity Act
Cybersecurity Certification Framework

- Established to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services, ICT processes and managed security services
- Provide for a mechanism to establish European cybersecurity certification schemes
- Shall attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle
- Shall attest that managed security services that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and confidentiality of data, which are accessed, processed, stored or transmitted in relation to the provision of those services, and that those services are provided continuously with the requisite competence, expertise and experience by staff with a very high level of relevant technical knowledge and professional integrity

EU Cybersecurity Act
Cybersecurity Certification Framework
Union rolling work programme

- Identify strategic priorities for future European cybersecurity certification schemes
- Includes a list of ICT products, ICT services and ICT processes or categories thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme
- Inclusion of specific ICT products, ICT services and ICT processes or categories thereof, or of managed security services, in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:
  - The availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services, ~~or~~ ICT processes or managed security services and, in particular, as regards the risk of fragmentation;
  - relevant Union or Member State law or policy;
  - market demand;
  - developments in the cyber threat landscape;
  - Request for the preparation of a specific candidate scheme by the ECCG

EU Cybersecurity Act
Cybersecurity Certification Framework
Security Objectives of Cybersecurity Certification Schemes
For ICT product, ICT service or ICT process

- Protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process
- Protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process
- Authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer
- Identify and document known dependencies and vulnerabilities
- Record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom
- Make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom
- Verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities
- Restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident
- ICT products, ICT services and ICT processes are secure by default and by design
- ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates

EU Cybersecurity Act
Cybersecurity Certification Framework
Security Objectives for Managed Security Services

- Ensure that the managed security services are provided with the requisite competence, expertise and experience, including that the staff in charge of providing these services has a very high level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;
- Ensure that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a very high level of quality at all times;
- Protect data accessed, stored, transmitted or otherwise processed in relation to the provision of managed security services against accidental or unauthorised access, storage, disclosure, destruction, other processing, or loss or alteration or lack of availability;
- Ensure that the availability and access to data, services and functions is restored in a timely manner in the event of a physical or technical incident;
- Ensure that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- Record, and enable to assess, which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- Ensure that the ICT products, ICT services and ICT processes [and the hardware] deployed in the provision of the managed security services are secure by default and by design, do not contain known vulnerabilities and include the latest security updates

EU Cybersecurity Act
Cybersecurity Certification Framework
Assurance Levels for Cybersecurity Certification Schemes

- A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services, ICT processes and managed security services: 'basic', 'substantial' or 'high'
  - Shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process or managed security service, in terms of the probability and impact of an incident
- European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity certification scheme under which the European cybersecurity certificate or EU statement of conformity is issued
- Security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme
  - Include the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service, ICT process or managed security service is to undergo
- Certificate or the EU statement of conformity shall refer to applicable technical specifications, standards and procedures
- European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Each of the evaluation levels shall correspond to one of the assurance levels and shall be defined by an appropriate combination of assurance components

EU Cybersecurity Act
Cybersecurity Certification Framework
Assurance Levels for Cybersecurity Certification Schemes

European cybersecurity certificate that refers to assurance level ‘basic’:

- Shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks
- The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken

European cybersecurity certificate that refers to assurance level ‘substantial’:

- Shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to **minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources**
- The evaluation activities to be undertaken shall include at least the following: **a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities**. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken

EU Cybersecurity Act
Cybersecurity Certification Framework
Assurance Levels for Cybersecurity Certification Schemes

European cybersecurity certificate that refers to assurance level ‘high’:

- Shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to **minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources**
- The evaluation activities to be undertaken shall include at least the following: **a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing**. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken

EU Cybersecurity Act
Cybersecurity Certification Framework
Conformity Self-Assessment

- A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services
- Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes and managed security services that present a low risk corresponding to assurance level ‘basic’
- Manufacturer or provider of ICT products, ICT services, ICT processes or managed security services may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated and shall assume responsibility for the compliance of the ICT product, ICT service, ICT process or managed security services with the requirements set out in that scheme.
- Manufacturer or provider of ICT products, ICT services,ICT processes or managed security services shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services or managed security services with the scheme available to the national cybersecurity certification authority for the period provided for in the corresponding European cybersecurity certification scheme

EU Cybersecurity Act
Cybersecurity Certification Framework
Cybersecurity Certification Scheme Elements

A European cybersecurity certification scheme shall include at least the following elements:

- The subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services, ICT processes and managed security services covered
- A clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme
- References to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme
- Where applicable, one or more assurance levels
- An indication of whether conformity self-assessment is permitted under the scheme
- Where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements
- The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved

EU Cybersecurity Act
Cybersecurity Certification Framework
Cybersecurity Certification Scheme Elements

A European cybersecurity certification scheme shall include at least the following elements:

- Where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant
- Where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;
- Rules for monitoring compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates or the EU statements of conformity
- Where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification
- Rules concerning the consequences for ICT products, ICT services, ICT processes and managed security services that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme
- Rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services, ICT processes and managed security services are to be reported and dealt with;
- Where applicable, rules concerning the retention of records by conformity assessment bodies

EU Cybersecurity Act
Cybersecurity Certification Framework
Cybersecurity Certification Scheme Elements

A European cybersecurity certification scheme shall include at least the following elements:

- The identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels
- The content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued
- The period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services
- Maximum period of validity of European cybersecurity certificates issued under the scheme
- Disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme
- Conditions for the mutual recognition of certification schemes with third countries;
- Where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level ‘high’
- Format and procedures to be followed by manufacturers or providers of ICT products, ICT services, ICT processes and managed security services in supplying and updating the supplementary cybersecurity information

EU Cybersecurity Act
Cybersecurity Certification Framework
Cybersecurity Certification

- ICT products, ICT services, ICT processes and managed security services that have been certified under a European cybersecurity certification scheme shall be presumed to comply with the requirements of such scheme
- Cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law
- Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law
- Conformity assessment bodies shall issue European cybersecurity certificates to assurance level ‘basic’ or ‘substantial’ on the basis of criteria included in the European cybersecurity certification scheme
- Where a European cybersecurity certification scheme requires an assurance level ‘high’, the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in certain cases, by a conformity assessment body
- The holder of a European cybersecurity certificate shall inform the appropriate authority or body of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service, ICT process or managed security services that may have an impact on its compliance with the requirements related to the certification.
- A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met
- A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States

EU Cybersecurity Act
Cybersecurity Certification Framework
National cybersecurity certification authorities

- Each Member State shall designate one or more national cybersecurity certification authorities in its territory and inform the Commission of its identity
- Shall be independent of the entities it supervises in its organisation
- Shall ensure that the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to the AI Act are strictly separated from their supervisory activities set out in the AI Act
- Member States shall ensure that national cybersecurity certification authorities have adequate resources to exercise their powers and to carry out their tasks in an effective and efficient manner
- National cybersecurity certification authorities should participate in the ECCG in an active, effective, efficient and secure manner
-

EU Cybersecurity Act
Cybersecurity Certification Framework
National cybersecurity certification authorities - Tasks

- Supervise and enforce rules included in European cybersecurity certification schemes for the monitoring of the compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates that have been issued in their respective territories
- Monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services that are established in their respective territories and that carry out conformity self-assessment
- Monitor compliance with and enforce the obligations of such manufacturers or providers set out in this act and in the corresponding European cybersecurity certification scheme
- Actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies
- Monitor and supervise the activities of the public bodies
- Where applicable, authorise conformity assessment bodies in accordance with the Regulation and restrict, suspend or withdraw existing authorisation where conformity assessment bodies infringe the requirements of this Regulation
- Handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies

EU Cybersecurity Act
Cybersecurity Certification Framework
National cybersecurity certification authorities - Tasks

- Investigate the subject matter of such complaints to the extent appropriate, and inform the complainant of the progress and the outcome of the investigation within a reasonable period
- Provide an annual summary report on the activities conducted
- Cooperate with other national cybersecurity certification authorities or other public authorities as necessary
- Monitor relevant developments in the field of cybersecurity certification

EU Cybersecurity Act
Cybersecurity Certification Framework
Peer Review

- National cybersecurity certification authorities shall be subject to peer review.
- Peer review shall assess:

1. Where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates are strictly separated from their supervisory activities and whether those activities are carried out independently from each other
2. The procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes and managed security services with European cybersecurity certificates
3. The procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services, ICT processes and managed security services
4. The procedures for monitoring, authorising and supervising the activities of the conformity assessment bodies
5. Where applicable, whether the staff of authorities or bodies that issue certificates for assurance level 'high'
6. Peer review shall be carried out by at least two national cybersecurity certification authorities of other Member States and the Commission and shall be carried out at least once every five years
7. The outcomes of peer reviews shall be examined by the ECCG

EU Cybersecurity Act
Cybersecurity Certification Framework
Conformity assessment bodies

- Conformity assessment bodies shall be accredited by national accreditation bodies
- Where a European cybersecurity certificate is issued by a national cybersecurity certification authority, the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body
- Where European cybersecurity certification schemes set out specific or additional requirements, only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes
- Accreditation shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed on the same conditions, provided that the conformity assessment body still meets the requirements set out in this Regulation
- National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation

EU Cybersecurity Act
Cybersecurity Certification Framework
European Cybersecurity Certifcation Group (ECCG)

- Composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities
- Tasks:
- Advise and assist the Commission in its work to ensure the consistent implementation and application of certifcations
- Assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme
- Adopt an opinion on candidate schemes prepared by ENISA
- Request ENISA to prepare candidate schemes
- Adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes
- Examine relevant developments in the field of cybersecurity certification and to exchange information and good practices on cybersecurity certification schemes
- Facilitate the cooperation between national cybersecurity certification authorities through capacity-building and the exchange of information
- Support implementation of peer assessment mechanisms;
- Facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards