Information and technology law course

LECTURE 7 – 16 OCTOBER 2024

FEDERICA CASAROSA – 2024/2025

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 (Cybersecurity Act) OJ L 151, 7.6.2019.

the Act is a combination of three factors.

- The first is the ambition to achieve a leading role in the global cybersecurity market.
- The second is the necessity to bridge the normative gaps created by the recent cyberattacks, whereby the law-maker realised that the current framework is unable to quickly respond to such threats.
- The third is the political opportunity to react to an emerging debate on the security of our information systems and networks and the geopolitical direction that the Union wants to take.

ENISA

Strenghtening the role of ENISA

Article 3 Mandate

1. ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders.

ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.

2. ENISA shall carry out the tasks assigned to it by Union legal acts that set out measures for approximating Member State laws, regulations and administrative provisions which are related to cybersecurity.

3. When carrying out its tasks, ENISA shall act independently while avoiding the duplication of Member State activities and taking into consideration existing Member State expertise.

4. ENISA shall develop its own resources, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.

ENISA – objectives

- Empowering Communities
- Cybersecurity Policy
- Operational Cooperation
- Capacity Building
- Trusted Solutions
- Foresight
- Knowledge

Certification schemes

Certification systems

Rec 69 Cybersecurity Act

- Therefore, it is necessary to adopt a common approach and to establish a **European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognised and used in all Member States**. In doing so, it is essential to build on existing national and international schemes, as well as on mutual recognition systems, in particular SOG-IS, and to make possible a smooth transition from the existing schemes under such systems to schemes under the new European cybersecurity certification framework. The European cybersecurity certification framework should have a twofold purpose. First, it should help increase trust in ICT products, ICT services and ICT processes that have been certified under European cybersecurity certification schemes. Second, it should help avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for undertakings operating in the digital single market. The European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, unless those standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in that regard.

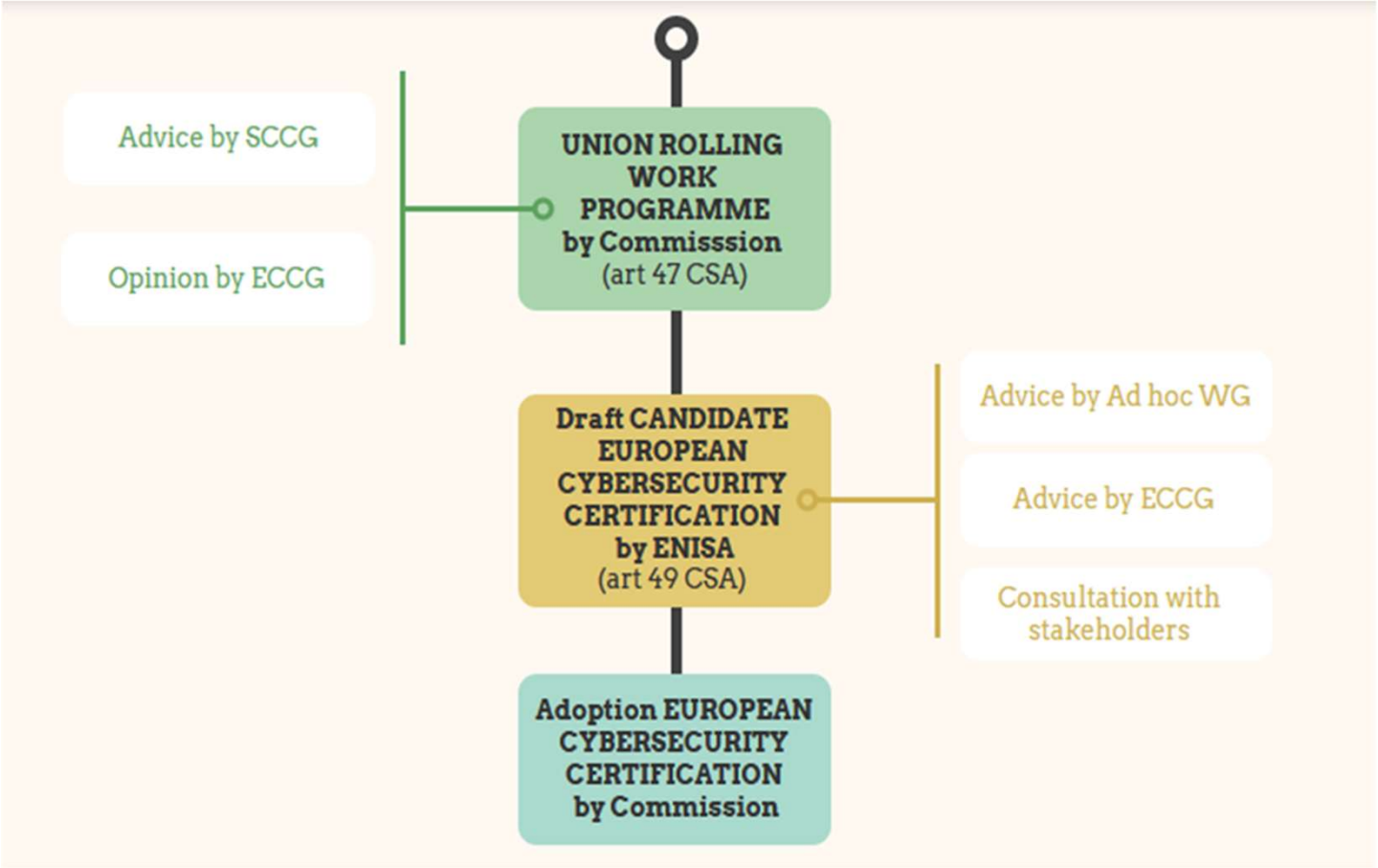
Certification schemes - definition

Art 2

(9) ‘European cybersecurity certification scheme’ means 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 or ICT processes;

(10) ‘national cybersecurity certification scheme’ means 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 and ICT processes falling under the scope of the specific scheme;

Certification schemes – procedure



Certification schemes – procedure

Art 47 The Union rolling work programme for European cybersecurity certification

- 3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof in the Union rolling work programme shall be justified **on the basis of one or more of the following grounds**:
  - (a) the availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services or ICT processes and, in particular, as regards the risk of fragmentation;
  - (b) relevant Union or Member State law or policy;
  - (c) market demand;
  - (d) developments in the cyber threat landscape;
  - (e) request for the preparation of a specific candidate scheme by the ECCG.
- 4. The Commission shall take due account of the opinions issued by the ECCG and the Stakeholder Certification Group on the draft Union rolling work programme.

Certification schemes – procedure

Article 51 Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:

- (a) to 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;
- (b) to 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;
- (c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- (d) to identify and document known dependencies and vulnerabilities;
- (e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
- (h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
- (i) that ICT products, ICT services and ICT processes are secure by default and by design;
- j) that 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.

Certification schemes – governance

Article 58 - National cybersecurity certification authorities

1. **Each Member State shall designate one or more national cybersecurity certification authorities in its territor**y or, with the agreement of another Member State, shall designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State. […]

3. Without prejudice to point (a) of Article 56(5) and Article 56(6), each national cybersecurity certification authority shall be **independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making. […]**

5. 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.

Certification schemes – governance

(97) Once a European cybersecurity certification scheme is adopted, **manufacturers or providers of ICT products, ICT services or ICT processes should be able to submit applications for certification** of their ICT products or ICT services to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a **maximum of five years and should be renewable on the same conditions** provided that the conformity assessment body still meets the requirements. **National accreditation bodies should 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.

Certification schemes – conformity assessment

Art 53

1. 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 or ICT processes. **Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.**

2. The manufacturer or provider …may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider …shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme.

3. T**he manufacturer or provider …shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products or ICT services with the scheme available to the national cybersecurity certification autho**rity referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

4. The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.

5. EU statements of conformity shall be recognised in all Member States.

Certification schemes

Centralised system

Granular system

Legal effect

Proposal for a revision of the Cybersecurity Act

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services

COM/2023/208 final

Main change

- Inclusion of managed security services (service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy) also as a subject for certification schemes

Proposal for a revision of the Cybersecurity Act

‘Article 51a Security objectives of European cybersecurity certification schemes for managed security services

A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives:

- (a) 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;
- (b) 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 ;
- (c) 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;
- (d) 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;
- (e) ensure that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- (f) record, and enable to assess, which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (g) 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;’;