Cybersecurity Law

HANDOUT – THE CYBERSECURITY PACKAGE

Proposal for a **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')**

Article 43 European cybersecurity certification schemes

A European cybersecurity certification scheme shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise 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, processes, services and systems.

Article 44

Preparation and adoption of a European Cybersecurity Certification Scheme

1. Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.

2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary.

3. ENISA shall transmit the candidate European cybersecurity certification scheme prepared in accordance with paragraph 2 of this Article to the Commission.

4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.

5. ENISA shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes.

Article 48 Cybersecurity certification

1. ICT products and services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 44 shall be presumed to be compliant with the requirements of such scheme.

2. The certification shall be voluntary, unless otherwise specified in Union law.

3. A European cybersecurity certificate pursuant to this Article shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44.

4. By the way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such public body shall be one of the following:

(a) a national certification supervisory authority referred to in Article 50(1)

(b) a body that is accredited as conformity assessment body pursuant to Article 51(1) or

(c) a body established under laws, statutory instruments, or other official administrative procedures of a Member State concerned and meeting the requirements for bodies certifying products, processes and services further to ISO/IEC 17065:2012.

5. The natural or legal person which submits its ICT products or services to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure.
6. Certificates shall be issued for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.
7. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.

Article 49 National cybersecurity certification schemes and certificates

1. Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant Article 44(4). Existing national cybersecurity certification schemes and the related procedures for the ICT products and services not covered by a European cybersecurity certification scheme shall continue to exist.
2. Member States shall not introduce new national cybersecurity certification schemes for ICT products and services covered by a European cybersecurity certification scheme in force.
3. Existing certificates issued under national cybersecurity certification schemes shall remain valid until their expiry date.

Proposal for a **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters**

Article 2 Definitions

For the purpose of this Regulation, the following definitions apply:
(a) 'European Production Order' means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence;
(b) 'European Preservation Order' means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production;
(c) 'service provider' means any natural or legal person that provides the following categories of services:
    (1) electronic communications service as defined in Article 2(4) of [Directive establishing the European Electronic Communications Code];
    (2) information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 that store data as part of the service provided to the user, including social networks, online marketplaces facilitating peer-to-peer transactions and other hosting service providers;
    (3) services that provide internet infrastructure such as IP address and domain name registries, domain name registrars and associated privacy and proxy services.
(d) 'offering services in the Union' means:
    (1) enabling legal or natural persons in one or more Member State(s) to use the services listed under c) above; and
    (2) establishing a real and substantial connection to the Member States referred to in point (1);
(e) 'electronic evidence' means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in subscriber and access data, transactional data and content data stored;