Cybersecurity Law

HANDOUT – THE NIS DIRECTIVE

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

Article 2 Objectives

1. The Agency shall develop and maintain a high level of expertise.
2. The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
3. The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
4. The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
5. The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Article 1 Subject matter and scope

1. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.
2. To that end, this Directive:

(a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;

(b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;

(c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;

(d) establishes security and notification requirements for operators of essential services and for digital service providers;

(e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

Article 5 Identification of operators of essential services

1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.
2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
(b) the provision of that service depends on network and information systems; and
(c) an incident would have significant disruptive effects on the provision of that service.

Article 6 Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors:
(a) the number of users relying on the service provided by the entity concerned;
(b) the dependency of other sectors referred to in Annex II on the service provided by that entity;
(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
(d) the market share of that entity;
(e) the geographic spread with regard to the area that could be affected by an incident;
(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.
2. In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors.

Annex III – categories

Energy
Transport
Banking
Financial market infrastructures
Health sector
Drinking water distribution
Digital infrastructure

Annex I – digital services

1. Online marketplace.
2. Online search engine.
3. Cloud computing service.

Article 4 Definitions

For the purposes of this Directive, the following definitions apply:
(17) 'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (18) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;
(18) 'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;
(19) 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.