High common level of network and information security across the Union. NIS Directive

2013/0027(COD) - 06/07/2016 - Final act

PURPOSE: ensure a high common level of security of network and information systems across the Union.

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

CONTENT: the 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. Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

However, the existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union.

Obligations with regard to their national cybersecurity capabilities: the Directive requires Members States to:

- adopt an **national strategy** and designate a **national authority on security of network and information systems** (NIS) with adequate resources to prevent, handle and respond to NIS risks and incidents;
- establish a network of the national **Computer Security Incident Response Teams** (CSIRTs) responsible for handling incidents and risks.

Cooperation: in order to support strategic cooperation among Member States, to develop trust and confidence and with a view to achieving a high common level of security of networks and information systems in the Union, the Directive provides for the establishment of a **Cooperation Group** which will be composed of representatives from the Member States, the Commission and the European Union Agency for Network and Information Security ('ENISA'). This Group will have specific tasks, such as exchanging best practices and information on a number of issues or discussing capabilities and preparedness of Member States.

In order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation, the Directive establishes a **network of the national CSIRTs.**

Security and notification requirements: the Directive aims to promote a **culture of risk management** and encourage the sharing of information between the public and private sectors.

Companies operating in certain critical sectors as well as public administrations must evaluate the risks they run and adopt appropriate and proportionate measures to ensure NIS. These companies must notify competent authorities of all incidents that seriously compromise their networks and information systems and have a significant disruptive effect on the continuity of critical services and supply of goods.

The requirement to notify security incidents affects:

- **operators of essential services** in sectors such as financial services, transport, energy and health;
- **providers of digital services** providing three types of services: (i) online market places, (ii) online search engines and (iii) cloud computing services;
- **public administrations** which are identified as operators of essential services.

Taking a **differentiated** approach with regard to the two categories of players, the Directive provides that the security and notification requirements are lighter for digital service providers than for operators of essential services.

ENTRY INTO FORCE: 8.8.2016.

TRANSPOSITION: by 9.5.2018.

APPLICATION: from 10.5.2016.