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

2013/0027(COD) - 17/05/2016 - Council position

The Council adopted its **position at first reading** with a view to the adoption of a Directive 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.

The proposed Directive lays down measures with a view to achieving a high common level of security of networks and information systems within the European Union so as to improve the functioning of the internal market.

The main elements of the compromise reached with the European Parliament are outlined below:

Obligations with regard to their national cybersecurity capabilities: under the Council position, Member States are required to:

adopt a **national strategy** defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of networks and information system;

- **designate one or more national competent authorities** on the security of network and information systems to monitor the application of the Directive at national level;
- **designate a national single point of contact** on the security of networks and information systems that will exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the cooperation group and the CSIRTs network. The single point of contact will also submit a yearly report on notifications received to the Cooperation Group;
- **designate one or more Computer Security Incident Response Teams** ("CSIRTs ") responsible for handling incidents and risks. The compromise text provides for requirements and tasks of CSIRTs in its Annex I.

Cooperation: in order to support and facilitate 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 Council position:

- **establishes 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') and will have specific tasks listed in the text, such as exchanging best practices and information on a number of issues or discussing capabilities and preparedness of Member States;
- **establishes a network of the national CSIRTs** in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation. The text provides for a list of tasks to be carried out by the network, such as exchanging information on CSIRTs services, operations and cooperation capabilities, supporting Member States in addressing cross border incidents or, under certain conditions, exchanging and discussing information related to incidents and associated risks.

Security and notification requirements: under the Council position, the Directive shall lay down certain obligations for two sets of market players: (i) **operators of essential services** and (ii) **digital service providers**.

The Directive takes a **differentiated approach** with regard to the two categories of players. The security and notification requirements are lighter for digital service providers than for operators of essential services, which reflects the degree of risk that disruption to their services may pose to society and economy.

Member States should be adequately equipped, in terms of both **technical and organisational capabilities** , to prevent, detect, respond to and mitigate network and information systems' incidents and risks.

Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide.

Essential services (Annex II) of the Directive lists a number of sectors important for society and economy, namely energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure. Within these sectors Member States will identify the operators of essential services, based on precise criteria provided for in the Directive.

Digital services (Annex III) of the Directive lists **three types of digital services**, the providers of which will have to comply with the requirements of the Directive: online market places, online search engines and cloud computing services. All digital service providers providing the listed services will have to comply with the requirements of the Directive with the exclusion of micro and small enterprises.

Entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

Transposition: Member States will be required to transpose the Directive by 21 months after the date of its entry into force and will have 6 additional months to identify their operators of essential services.