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

2013/0027(COD) - 13/03/2014 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 521 votes to 22 with 25 abstentions, a legislative resolution on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security (NIS) across the Union.

Parliament's position in first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Scope: the draft Directive aims at imposing obligations on public administrations and market operators, including critical infrastructures and information society services.

In order to achieve proportionality and swift results of the Directive, Members consider that the compulsory measures laid down in Chapter IV should be limited to infrastructures that are critical in a stricter sense. They took the view that **information society services should therefore not be included** in the list of market operators in Annex II of the draft directive (such as internet payment gateways, social networks, search engines, cloud computing services).

The Directive should **focus on critical infrastructure essential for the maintenance of vital economic and societal activities** in the fields of energy, transport, banking, financial market infrastructures and health. Software developers and hardware manufacturers should be excluded from the scope of this Directive.

Protection and processing of personal data: Members stressed that any processing of personal data in the Member States pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC and Directive 2002/58/EC. Any use of personal data should be limited only to what is necessary and should be as anonymous as possible, or even totally anonymous.

National NIS strategies: Parliament proposed that Member States may request the assistance of the **European Union Agency for Network and Information Security** (ENISA) in developing their national NIS strategies and national NIS cooperation plans, based on a common minimum NIS strategy.

National competent authorities and single points of contact on the security of network and information systems: Members proposed amending the directive to authorise the designation of **one or more competent authorities** by Member States.

However, in order to ensure a coherent application within the Member State and in order to allow for an effective and streamlined cooperation at Union level, each Member State should appoint one **single point of contact**. The single point of contact shall ensure, among other things, cross-border cooperation with other single points of contact.

Computer Emergency Response Teams (CERTs): each Member State shall set up **at least one** Response Team for each of the sectors established in Annex II, responsible for handling incidents and risks according to a well-defined process.

CERTs should have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks.

CERTs will be encouraged to initiate and to participate in joint exercises with other CERTs, with all Member States-CERTs, and with appropriate institutions of non-Member States as well as with CERTs of multi- and international institutions such as NATO and the United Nations.

Cooperation network: with the aim of strengthening the activities of the cooperation network, Members consider that the latter should envisage inviting market operators and suppliers of cyber security solutions to participate where appropriate. The cooperation network shall publish a report once a year on the activities of the network.

Member States may determine **the level of criticality of market operators**, taking into account the specificities of sectors, and different parameters.

The Commission shall adopt, by means of delegated acts, a **common set of interconnection and security standards** that single points of contact are to meet before exchanging sensitive and confidential information across the cooperation network.

Security requirements and incident notification: the proposal provides that the Commission shall be empowered to adopt delegated acts concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.

For the purpose of clarifying the scope of obligations and enshrining them in the basic act, it is proposed to **replace the delegated acts with clear criteria** to determine the significance of incidents to be reported. To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account: i) the number of users whose core service is affected; ii) the duration of the incident; iii) the geographic spread with regard to the area affected by the incident.

After consultation with the notified competent authority and the market operator concerned, the single point of contact may **inform the public** about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an ongoing incident. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis.

Implementation and enforcement: the proposal provides that market operators provide an audit carried out by a qualified independent body or national authority, and make the evidence available to the competent authority. Parliament suggested **allowing for flexibility regarding the evidence for compliance** with the security requirements imposed on market operators by admitting proof of compliance provided in a form other than security audits.

The single points of contact and the data protection authorities shall develop, in cooperation with ENISA, **information exchange mechanisms and a single template** to be used both for notifications.

Sanctions: Members proposed clarifying that where the market operator has failed to comply with the obligations in relation to the directive, but has not acted with intent or gross negligence, no sanction should be imposed.