Council of the EU

PRESS
EN

PRESS RELEASE
538/15
29/06/2015

Network and information security: breakthrough in talks with EP

On 29 June 2015, the Latvian presidency of the Council reached an **understanding with the European Parliament on the main principles** to be included in the draft directive on **network and information security (NIS)**. These principles will then need to be turned into legal provisions to allow for a final deal on the directive at a later stage. The presidency will present the outcome of this fourth trilogue to member states' ambassadors at the meeting of the Permanent Representatives Committee on 30 June.

"The rise of cyber attacks is one of the greatest threats we are facing, and today's agreement on the global package is a big step towards the finalisation of the first EU-wide measures to counter this threat", said Raimonds Vējonis, the Latvian Minister for Defence. "This also reflects the priority given to this issue by EU leaders, who on Friday called for rapid adoption of the directive."

Stronger cyber risk management and incident reporting across the EU

The new rules will require designated operators that provide **essential services** (in areas such as energy and transport) to take measures to manage risks to their networks and report incidents to authorities. Member states will identify such essential operators to be covered by the directive, based on clear criteria laid down in the text. Particular provisions will be introduced to avoid fragmentation in the identification of operators across member states. However, these are not to undermine member states' prerogatives or security concerns.

It was agreed that **digital service platforms** would be treated in a different manner from essential services. The details will be discussed at a technical level.

Member states will be required to establish a NIS plan and designate competent authorities. An EU-level cooperation group will be created to address NIS matters at a **strategic** level and guide operational activities. For such **operational** cooperation, a network of national Computer Security Incident Response Teams (CSIRTs) will be set up. It will help develop confidence and trust between member states.

What benefits is the NIS directive expected to bring?

The NIS proposal aims to ensure a **secure and trustworthy digital environment** throughout the EU. **Citizens** and consumers will have more trust in the technologies, services and systems they rely on day-to-day. This increased confidence will mean a more inclusive cyberspace, and a digital economy that grows even faster, supporting economic recovery. **Governments and businesses** will be able to rely more on digital networks and infrastructure to provide their essential services at home and across borders. More secure e-commerce platforms could bring more customers online and create new opportunities. **Providers** of ICT security products and services would also benefit, as demand for their products and services is bound to increase, leading to innovative products and economies of scale. The **EU economy** will benefit as sectors that rely heavily on NIS will be better supported to offer a more reliable service.

How will it become a law?

The presidency negotiates the terms of the directive with the European Parliament on behalf of the Council. In order to be adopted, the legal act must be approved by both institutions. The talks will continue under the incoming Luxembourg presidency.

- Improving cyber security across the EU

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press