

PRESS RELEASE

904/15

08/12/2015

First EU-wide rules to improve cybersecurity: deal with EP

On 7 December 2015, the Luxembourg presidency of the Council reached an informal agreement with the European Parliament on common rules to strengthen **network and information security** (NIS) across the EU.

The new directive will set out cybersecurity obligations for **operators of essential services** and **digital service providers**. These operators will be required to take measures to manage cyber risks and report major security incidents, but the two categories will be subject to different regimes.

Xavier Bettel, Luxembourg's Prime Minister and Minister for Communications and the Media, and President of the Council, said: "This is an important step towards a more coordinated approach in cybersecurity across Europe. All actors, public and private, will have to step up their efforts, in particular by increased cooperation between member states and enhanced security requirements for infrastructure operators and digital services".

Stronger rules for essential operators

The directive lists a number of **critical sectors** in which operators of essential services are active, such as energy, transport, finance and health. Within these sectors, member states will identify the operators providing essential services, based on clear criteria laid down in the directive. The requirements and supervision will be stronger for these operators than for providers of digital services. This reflects the degree of risk that any disruption to their services may pose to society and the economy.

A more uniform regime for digital service providers

The following digital services will be covered by the directive: **e-commerce platforms, search engines and cloud services**.

Digital service providers are typically active in many member states. To ensure that they are treated in a similar way across the EU, the rules will apply to all operators providing such services, with the exclusion of small companies.

National and EU-level frameworks to counter cyber threats

Each EU country will be required to designate one or more national authorities and set out a strategy to deal with cyber matters.

Member states will also step up their cooperation on cybersecurity. An EU-level cooperation group will be created to support strategic cooperation and exchange of best practices among member states. A network of national computer security incident response teams (CSIRTs) will be set up to promote operational cooperation. Both are also expected to help develop confidence and trust between member states.

Deadlines

Member states will have 21 months from the directive's entry into force to adopt the necessary national provisions. Following this period, they will have 6 further months to identify their operators of essential services.

How will it become law?

For the Council, the deal still has to be confirmed by member states. The presidency will present the agreed text for approval by member states' ambassadors at the Permanent Representatives Committee (Coreper) on 18 December. To conclude the procedure, formal adoption by both the Council and the Parliament is required.

- [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

