European Commission - Press release

Commission welcomes political agreement on new rules on cybersecurity of network and information systems

Brussels, 13 May 2022

The Commission welcomes the political agreement reached today between the European Parliament and EU Member States on the **Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)** proposed by the Commission in December 2020.

The existing rules on the security of network and information systems (NIS Directive), have been the first piece of EU-wide legislation on cybersecurity and paved the way for a significant change in mind-set, institutional and regulatory approach to cybersecurity in many Member States. In spite of their notable achievements and positive impact, they had to be updated because of the increasing degree of digitalisation and interconnectedness of our society and the rising number of cyber malicious activities at global level.

To respond to this increased exposure of Europe to cyber threats, the **NIS 2 Directive** now covers medium and large entities from more sectors that are critical for the economy and society, including providers of public electronic communications services, digital services, waste water and waste management, manufacturing of critical products, postal and courier services and public administration, both at central and regional level. It also covers more broadly the healthcare sector, for example by including medical device manufacturers, given the increasing security threats that arose during the COVID-19 pandemic. The expansion of the scope covered by the new rules, by effectively obliging more entities and sectors to take cybersecurity risk management measures, will help increase the level of cybersecurity in Europe in the medium and longer term.

The NIS 2 Directive also strengthens cybersecurity requirements imposed on the companies, addresses security of supply chains and supplier relationships and introduces accountability of top management for non-compliance with the cybersecurity obligations. It streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, as well as stricter enforcement requirements, and aims at harmonising sanctions regimes across Member States. It will help increase information sharing and cooperation on cyber crisis management at a national and EU level.

Members of the College said:

Margrethe **Vestager**, Executive Vice-President for a Europe Fit for the Digital Age, said: *"We have been working hard for digital transformation of our society. In the past months we have put a number of building blocks in place, such as the Digital Markets Act and the Digital Services Act. Today, Member States and the European Parliament have also secured an agreement on NIS 2. This is another important breakthrough of our European digital strategy, this time to ensure that citizens and businesses are protected and trust essential services."*

Margaritis **Schinas**, Vice-President for Promoting our European Way of Life, said: "*Cybersecurity was always essential to shield our economy and our society against cyber threats; it is becoming critical as we are moving further in the digital transition. The current geopolitical context makes it even more urgent for the EU to ensure that its legal framework is fit for purpose. By agreeing on these further strengthened rules, we are delivering on our commitment to enhance our cybersecurity standards in the EU. Today, the EU shows its clear determination to champion preparedness and resilience against cyber threats, which target our economies, our democracies and peace."*

Thierry **Breton**, Commissioner for the Internal Market, said: *"Cyber threats have become bolder and more complex. It was imperative to adapt our security framework to the new realities and to make sure our citizens and infrastructures are protected. In today's cybersecurity landscape, cooperation and rapid information sharing are of paramount importance. With the agreement of NIS2, we modernise rules to secure more critical services for society and economy. This is therefore a major step forward. We will complement this approach with the upcoming Cyber Resilience Act that will ensure that digital products are also more secure whenever they are used."*

Next Steps

The political agreement reached by the European Parliament and the Council is now subject to formal approval by the two co-legislators. Once published in the Official Journal, the Directive will enter into force 20 days after publication and Member States will then need to transpose the new elements of the Directive into national law. Member States will have 21 months to transpose the Directive into national law.

Background

Cybersecurity is one of the Commission's top priorities and a cornerstone of the digital and connected Europe.

The first EU-wide law on cybersecurity, the NIS Directive, that came into force in 2016 helped to achieve a common high level of security of network and information systems across the EU. As part of its key policy objective to make Europe fit for the digital age, the Commission proposed the revision of the NIS Directive in December 2020. The EU Cybersecurity Act that is in force since 2019 equipped Europe with a framework of cybersecurity certification of products, services and processes and reinforced the mandate of the EU Agency for Cybersecurity (ENISA).

For More Information

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient

Factsheet on the new EU Cybersecurity Strategy

Factsheet on the Proposal for a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive)

Questions and Answers: New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient

IP/22/2985

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email