Fighting cybercrime: new EU cybersecurity laws explained

Parliament has passed new laws strengthening EU cybersecurity in key sectors. Find out how they will protect you.

Parliament approves cybercrime measures

With the rapidly expanding digitalisation of daily life, further accelerated by the Covid-19 pandemic, protection against cyber threats has become essential for society to function properly.

Cyberattacks can prove very costly. According to the European Commission, the annual cost of cybercrime to the global economy is estimated to have reached €5.5 trillion by the end of 2020.

In November 2022, the European Parliament updated EU law to bolster investment in strong cybersecurity for essential services and critical infrastructure and strengthen EU-wide rules.

Parliament also boosted the protection of the EU's essential infrastructure, including digital infrastructure, on 22 November 2022, giving its final approval to legislation tightening the risk assessments and reporting requirements for critical organisations in 11 essential sectors.

Read more about how the EU shapes the digital transformation
Tightening cybersecurity obligations - the NIS2 directive

The Network and Information Security directive (NIS2) introduces new rules to advance a high common level of cybersecurity across the EU – both for companies and countries. It also strengthens cybersecurity requirements for medium-sized and large entities that operate and provide services in key sectors.

An update of the 2016 NIS directive, it aims to improve clarity and implementation, as well as address fast-paced developments in this area. It covers more sectors and activities than before, streamlines reporting obligations and addresses supply chain security.

After approval by Parliament and EU countries in the Council in November 2022, member states have 21 months to implement it.

Find out what the main and emerging cyber threats are

More sectors included

The new law expands the scope of sectors and activities that are critical for the economy and society, including energy, transport, banking, health, digital infrastructure, public administration and space. However, it does not cover national and public security, law enforcement or the judiciary. The law applies to public administration at central and regional level, but not parliaments and central banks.

It requires more entities and sectors to take cybersecurity risk management measures, including providers of public electronic communications services, social media operators, manufacturers of critical products (including medical devices), and postal and courier services.

Stricter obligations for countries

The law sets stricter cybersecurity obligations for EU countries when it comes to supervision. It improves the enforcement of those obligations, including by harmonising sanctions across member states. It also aims to improve cooperation between EU countries, including on large-scale incidents, under the umbrella of the EU Agency for Cybersecurity (Enisa).

Cyber Resilience Act: boosting security of digital products
More and more everyday products have a digital component - for example baby monitors, connected doorbells or wifi routers - which makes them susceptible to cyber-attacks. To make sure that they are safe, Parliament approved the Cyber Resilience Act, which provides a uniform set of mandatory, EU-wide cybersecurity requirements for products connected to another device or a network.

During negotiations on the final shape of the law with EU countries in the Council, MEPs made sure that the list of systems and products that will have to meet stricter security requirements includes private security cameras, baby monitors, smart home assistants, smart watches and smart toys. Security updates will be installed automatically and separately from functional updates.

Digital Operational Resilience Act: protecting the EU’s financial system

Because the financial sector is more and more dependent on software and digital processes, it also needs increased protection. The Digital Operational Resilience Act (Dora) will ensure that the EU’s financial sector is more resilient to severe operational disruptions and cyber-attacks. Parliament gave final approval to the legislation, previously agreed with the Council, on 10 November 2022. The Council formally approved the regulation on 28 November 2022.

The law introduces and harmonises digital operational resilience requirements for the EU’s financial services sector, obliging companies to make sure that they can withstand, respond to and recover from all types of information and communication technology (ICT) related disruptions and threats.

The new rules apply to all companies providing financial services - such as banks, payment providers, electronic money providers, investment firms, crypto-asset service providers as well as to critical ICT third-party service providers.

National authorities will supervise and enforce implementation.

Read more about how the EU is shaping the digital transformation

- Artificial intelligence rules
• European strategy for data
• Digital Markets Act/Digital Services Act
• Dangers of cryptocurrency
• Microchips shortage crisis

New EU rules aim to protect key sectors such as health better against cyber attacks.

Network and Information Security directive (NIS2)
Check legislative progress
Briefing

Cyber Resilience Act
Check legislative progress
Briefing

Digital Operational Resilience Act
Check legislative progress
Briefing

More on cybersecurity and digital finance
European Commission welcomes political agreement on new rules on cybersecurity of network and information systems
Digital finance: introduction and timeline