A high common level of cybersecurity

2020/0359(COD) - 16/12/2020 - Legislative proposal

PURPOSE: to introduce new measures for a common level of cybersecurity across the EU.

PROPOSED ACT: Directive of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: Directive (EU) 2016/1148 of the European Parliament and the Council aimed at building cybersecurity capabilities across the EU, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the EU's economy and society to function effectively.

However, since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union’s level of cybersecurity resilience.

CONTENT: this proposal builds on and repeals Directive (EU) 2016/1148 on security of network and information systems (NIS Directive), which is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the EU. The proposal modernises the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape.

Specific provisions

Scope

The proposal should apply to certain public or private essential entities operating in the sectors listed in Annex I (energy; transport; banking; financial market infrastructures; health, drinking water; waste water; digital infrastructure; public administration and space) and certain important entities operating in the sectors listed in Annex II (postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers).

Micro and small entities are excluded from the scope of the Directive, except for providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration, and certain other entities, such as the sole provider of a service in a Member State.

National cybersecurity frameworks

The proposal stipulates that Member States are required to adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity. The proposed directive also establishes a framework for Coordinated Vulnerability Disclosure and requires Member States to designate computer security incident response teams to act as trusted intermediaries and facilitate the interaction between the reporting entities and the manufacturers or providers of ICT products and ICT services.

Member States are required to put in place National Cybersecurity Crisis Management Frameworks, by designating national competent authorities responsible for the management of large-scale cybersecurity incidents and crises.

Cybersecurity risk management and reporting obligations

The proposal requires Member States to provide that management bodies of all entities under the scope to approve the cybersecurity risk management measures taken by the respective entities and to follow specific cybersecurity-related training. Member States are required to ensure that entities under the scope take appropriate and proportionate technical and organisational measures to manage the cybersecurity risks posed to the security of network and information systems.

TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data. Furthermore, such entities are required to provide efficient access to domain registration data for legitimate access seekers.

Jurisdiction and registration

As a rule, essential and important entities are deemed to be under the jurisdiction of the Member State where they provide their services. However, certain types of entities (DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers, as well as certain digital providers) are deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.

Information sharing

Member States should provide rules enabling entities to engage in cybersecurity-related information sharing within the framework of specific cybersecurity information-sharing arrangements.

Supervision and enforcement

Competent authorities are required to supervise the entities under the scope of the proposed directive, and in particular to ensure their compliance with the security and incident notification requirements. The proposal also requires Members States to impose administrative fines to essential and important entities and defines certain maximum fines.