# The contribution of the Union of Entrepreneurs and Employers to the European Commission's consultation on the Cyber Resilience Act - new cybersecurity rules for digital products and ancillary services

On 16 March 2022, the European Commission launched the public consultation on the Cyber Resilience Act - new cybersecurity rules for digital products and ancillary services.[1] The act was announced by the President of the European Commission Ursula von der Leyen in her State of the Union address, in September 2021.[2] Launching the consultation, the Commission also issued a call for evidence for an assessment of the impact of the regulations. The act on cyber resilience is to supplement the delegated regulation of 29 October 2021 issued under the Radio Equipment Directive by formulating optimised cybersecurity requirements covering a wide range of digital products and ancillary services.[3] Moreover, the regulations will supplement the existing legal framework, which includes the NIS Directive[4] and the EU Cybersecurity Act[5], and which will fit into the future NIS 2 Directive.[6]

The rationale for the consulted project is to prevent cyberattacks. The lack of adequate security features and insufficient response to vulnerabilities throughout the product lifecycle were identified as the cause of this situation. Moreover, the European Commission has pointed to the lack of sufficient information on product safety. The factors contributing to the lowering of security levels are the absence of economic incentives and the shortage of qualified experts on security.

The regulation aims to establish simplified security requirements covering a wide range of digital products and ancillary services. The new act is to regulate tangible digital products (wired as well as wireless) and non-embedded software, which will be subject to the provisions of the act throughout the lifecycle of the product.

According to the European Commission, the existing regulatory framework is insufficient, as it does not cover all digital products (e.g. non-embedded software) and does not specify detailed safety requirements covering the entire life cycle of products. Given the above, the Commission is considering various policy lines to prevent cyber threats, such as: ad hoc regulatory solutions within existing legislation, horizontal regulatory intervention, the adoption of voluntary measures (including the development of certification systems), a mixed regulatory approach, or maintaining the status quo.

The Union of Entrepreneurs and Employers welcomes the Commission's proposal aimed at improving the level of cyber security of European users. We have identified two key aspects that the proposed act seeks to regulate. The first is the assessment of security levels from the point of view of services provided to final users. It is understood as the security of users' data and the access (as well as the reliability of access) to the services provided, especially by public networks. The second is the protection

[1]https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_pl

[2] https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2021_pl

[3] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022R0030&from=PL

[4] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=BG

[5] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[6]https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

of public networks against threats related to cyberattacks. This should also include attacks from the inside of the networks, which may be caused by security gaps in software. The Polish Cybersecurity System Act and the regulatory framework it creates is also important in this context.[7]

According to the Union of Entrepreneurs and Employers, it is especially important to develop hardware and software for radio access networks. It needs to be pointed out that the access to the operator's RAN equipment is limited. The equipment is physically located at the operator's premises, where it is protected against third-party interference. Moreover, the devices operate within a dedicated operator network, which ensures the security of remote access. It protects this dedicated network against unauthorised access. Given the above, the operator is in full control of the access to RAN equipment.

User data security is described in the technical specification and operator settings relevant for the selected radio access technology (2G/3G/4G/5G). The technical specification determines encryption and security algorithms, and key lengths. This ensures that there are no differences between equipment suppliers in terms of providing security to both end users and the network itself.

In the view of the above, we believe that ensuring an adequate level of security should be the responsibility of operators who have the best-adapted tools to respond dynamically to arising threats. Similarly, in view of the existing security protection mechanisms applied by individual entities, we are in favour of maintaining the power to subject these entities to audits.

In our opinion, operators have the best knowledge of techniques to protect their own networks and have their best interest in maintaining the security of their own environments, which is confirmed by past practice. We recommend verifying whether the security solutions and algorithms proposed in the technical specification are sufficient to ensure the cyber security of digital products and ancillary services.

[7] https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf