Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[(1)],

Having regard to the opinion of the Committee of the Regions[(2)],

Acting in accordance with the ordinary legislative procedure[(3)],

Whereas:

(1) Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the functioning of the internal market.

(2) The use of network and information systems by citizens, organisations and businesses across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the internet of Things (IoT) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions. Network and

Changes to legislation: *Regulation (EU) 2019/881 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 28 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

information systems are capable of supporting all aspects of our lives and drive the Union's economic growth. They are the cornerstone for achieving the digital single market.

(3) Increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), as defined in Commission Recommendation 2003/361/EC[(4)], to operators of critical infrastructure – are better protected from cyber threats.

(4) By making the relevant information available to the public, the European Union Agency for Network and Information Security (ENISA), as established by Regulation (EU) No 526/2013 of the European Parliament and of the Council[(5)] contributes to the development of the cybersecurity industry in the Union, in particular SMEs and start-ups. ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union.

(5) Cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyberattacks often take place across borders, the competence of, and policy responses by, cybersecurity and law enforcement authorities are predominantly national. Large-scale incidents could disrupt the provision of essential services across the Union. This necessitates effective and coordinated responses and crisis management at Union level, building on dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of cybersecurity and resilience in the Union, based on reliable Union data, as well as systematic forecasts of future developments, challenges and threats, at Union and global level, are important for policy makers, industry and users.

(6) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and would foster mutually reinforcing objectives. Those objectives include further increasing the capabilities and preparedness of Member States and businesses, as well as improving cooperation, information sharing and coordination across Member States and Union institutions, bodies, offices and agencies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in cases of large-scale cross-border incidents and crises, while taking into account the importance of maintaining and further enhancing the national capabilities to respond to cyber threats of all scales.

(7) Additional efforts are also needed to increase citizens', organisations' and businesses' awareness of cybersecurity issues. Moreover, given that incidents undermine trust in digital service providers and in the digital single market itself, especially among

***Changes to legislation:** Regulation (EU) 2019/881 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 28 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

consumers, trust should be further strengthened by offering information in a transparent manner on the level of security of ICT products, ICT services and ICT processes that stresses that even a high level of cybersecurity certification cannot guarantee that an ICT product, ICT service or ICT process is completely secure. An increase in trust can be facilitated by Union-wide certification providing for common cybersecurity requirements and evaluation criteria across national markets and sectors.

(8) Cybersecurity is not only an issue related to technology, but one where human behaviour is equally important. Therefore, 'cyber-hygiene', namely, simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to risks from cyber threats, should be strongly promoted.

(9) For the purpose of strengthening Union cybersecurity structures, it is important to maintain and develop the capabilities of Member States to comprehensively respond to cyber threats, including to cross-border incidents.

(10) Businesses and individual consumers should have accurate information regarding the assurance level with which the security of their ICT products, ICT services and ICT processes has been certified. At the same time, no ICT product or ICT service is wholly cyber-secure and basic rules of cyber-hygiene have to be promoted and prioritised. Given the growing availability of IoT devices, there is a range of voluntary measures that the private sector can take to reinforce trust in the security of ICT products, ICT services and ICT processes.

(11) Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. In many cases, identifying and documenting such dependencies enables end users of ICT products, ICT services and ICT processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures.

(12) Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation.

(13) Undertakings, organisations and the public sector should configure the ICT products, ICT services or ICT processes designed by them in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible ('security by default'), thereby reducing the burden on users of having to configure an ICT product, ICT service or ICT process appropriately. Security by default should not require extensive configuration or specific technical

Changes to legislation: *Regulation (EU) 2019/881 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 28 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

understanding or non-intuitive behaviour on the part of the user, and should work easily and reliably when implemented. If, on a case-by-case basis, a risk and usability analysis leads to the conclusion that such a setting by default is not feasible, users should be prompted to opt for the most secure setting.

(14) Regulation (EC) No 460/2004 of the European Parliament and of the Council[(6)] established ENISA with the purposes of contributing to the goals of ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. Regulation (EC) No 1007/2008 of the European Parliament and of the Council[(7)] extended ENISA's mandate until March 2012. Regulation (EU) No 580/2011 of the European Parliament and of the Council[(8)] further extended ENISA's mandate until 13 September 2013. Regulation (EU) No 526/2013 extended ENISA's mandate until 19 June 2020.

(15) The Union has already taken important steps to ensure cybersecurity and to increase trust in digital technologies. In 2013, the Cybersecurity Strategy of the European Union was adopted to guide the Union's policy response to cyber threats and risks. In an effort to better protect citizens online, the Union's first legal act in the field of cybersecurity was adopted in 2016 in the form of Directive (EU) 2016/1148 of the European Parliament and of the Council[(9)]. Directive (EU) 2016/1148 put in place requirements concerning national capabilities in the field of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for the economy and society, such as energy, transport, drinking water supply and distribution, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces).
A key role was attributed to ENISA in supporting the implementation of that Directive. In addition, fighting effectively against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity. Other legal acts such as Regulation (EU) 2016/679 of the European Parliament and of the Council[(10)] and Directives 2002/58/EC[(11)] and (EU) 2018/1972[(12)] of the European Parliament and of the Council also contribute to a high level of cybersecurity in the digital single market.

(16) Since the adoption of the Cybersecurity Strategy of the European Union in 2013 and the last revision of ENISA's mandate, the overall policy context has changed significantly as the global environment has become more uncertain and less secure. Against that background and in the context of the positive development of the role of ENISA as a reference point for advice and expertise, as a facilitator of cooperation and of capacity-building as well as within the framework of the new Union cybersecurity policy, it is necessary to review ENISA's mandate, to establish its role in the changed cybersecurity ecosystem and to ensure that it contributes effectively to the Union's response to cybersecurity challenges emanating from the radically transformed cyber threat landscape, for which, as recognised during the evaluation of ENISA, the current mandate is not sufficient.

***Changes to legislation:** Regulation (EU) 2019/881 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 28 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(17) ENISA as established by this Regulation should succeed ENISA as established by Regulation (EU) No 526/2013. ENISA should carry out the tasks conferred on it by this Regulation and other legal acts of the Union in the field of cybersecurity, among other things, by providing advice and expertise and by acting as a Union centre of information and knowledge. It should promote the exchange of best practices between Member States and private stakeholders, offer policy suggestions to the Commission and the Member States, act as a reference point for Union sectoral policy initiatives with regard to cybersecurity matters, and foster operational cooperation, both between Member States and between the Member States and Union institutions, bodies, office and agencies.

(18) Within the framework of Decision 2004/97/EC, Euratom taken by common agreement between the Representatives of the Member States, meeting at Head of State or Government level[(13)], the representatives of the Member States decided that ENISA would have its seat in a town in Greece to be determined by the Greek Government. ENISA's host Member State should ensure the best possible conditions for the smooth and efficient operation of ENISA. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and for enhancing the efficiency of networking activities that ENISA be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of ENISA. The necessary arrangements should be laid down in an agreement between ENISA and the host Member State concluded after obtaining the approval of the Management Board of ENISA.

(19) Given the increasing cybersecurity risks and challenges the Union is facing, the financial and human resources allocated to ENISA should be increased to reflect its enhanced role and tasks, and its critical position in the ecosystem of organisations defending the digital ecosystem of the Union, allowing ENISA to effectively carry out the tasks conferred on it by this Regulation.

(20) ENISA should develop and maintain a high level of expertise and operate as a reference point, establishing trust and confidence in the single market by virtue of its independence, the quality of the advice it delivers, the quality of information it disseminates, the transparency of its procedures, the transparency of its methods of operation, and its diligence in carrying out its tasks. ENISA should actively support national efforts and should proactively contribute to Union efforts while carrying out its tasks in full cooperation with the Union institutions, bodies, offices and agencies and with the Member States, avoiding any duplication of work and promoting synergy. In addition, ENISA should build on input from and cooperation with the private sector as well as other relevant stakeholders. A set of tasks should establish how ENISA is to accomplish its objectives while allowing flexibility in its operations.

(21) In order to be able to provide adequate support to the operational cooperation between Member States, ENISA should further strengthen its technical and human capabilities and skills. ENISA should increase its know-how and capabilities. ENISA and Member