IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

COUNCIL

Council conclusions on the cybersecurity of connected devices

(2020/C 427/04)

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING:

— the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,

— the Council conclusions on cybersecurity capacity and capabilities building in the EU,

— the Council conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G,

— the Council conclusions on the future of a highly digitised Europe beyond 2020: 'Boosting digital and economic competitiveness across the Union and digital cohesion',

— the Council conclusions on shaping Europe's Digital Future,

— the European Council conclusions on COVID-19, the Single Market, industrial policy, digital and external relations,

— the Communication of the European Commission on shaping Europe's Digital Future,

1. HIGHLIGHTS that the European Union and its Member States need to ensure their digital sovereignty and strategic autonomy, while preserving an open economy. This includes reinforcing the ability to make autonomous technological choices and as one of the main pillars, resilient and secure infrastructures, products and services for building trust in the Digital Single Market and within the European society. The European Union's core values preserve in particular privacy, security, equality, human dignity, rule of law and open Internet as prerequisites for reaching a digital-driven human-centric society, economy and industry.

2. RECOGNISES the growing importance of connected devices and their security, including machines, sensors and networks that make up the Internet of Things (IoT). Connected devices will play a key role in further shaping Europe's digital future, from an industrial and business point of view, as well as in the daily life of consumers of a new generation of technology. In addition to 5G, artificial intelligence, quantum computing, high performance computing, cloud computing, distributed ledger technologies namely blockchain and any other new applications and opportunities for a sustainable economic growth and a higher level of digitalisation of our society can only be reached through cyber-secure connected devices.

3. NOTES that the increased usage of consumer products and industrial devices connected to the internet will also raise new risks for privacy, information- and cybersecurity, including increasingly potential impacts on the integrity and availability of products and data, which can directly affect safety. It is essential to minimise such risks in order to protect consumers, to strengthen Europe's overall cyber resilience and to enhance the trust of citizens in digital solutions and technologies. This will also foster the competitiveness and innovation capabilities of European

providers of such devices. Cybersecurity and privacy should be acknowledged as essential requirements in product innovation, the production and development processes, including the design phase (security by design), and should be ensured throughout a product's entire life cycle and across its supply chain.

4. EMPHASISES that in addition to ensuring a high level of security of connected devices, it is equally important to increase consumer awareness of their potential privacy and security risks. This would help to minimise threats stemming from increased usage of connected devices, enhance trust in the Digital Single Market and make most of economic and societal benefits that technologies of connected devices offer.

5. UNDERLINES that public investments in research and innovation, notably through Horizon Europe and Digital Europe, as well as private investments could create valuable incentives to make connected devices safer and more secure, and therefore smart communication networks more resilient. Investments in the necessary digital infrastructure and technology to deploy the latest technologies of connected devices should also be accelerated to achieve industrial and digital leadership, and to ensure strategic autonomy, while preserving an open economy.

6. STRESSES the need to ensure a high level of complementarity and comparability of security functionalities of ICT systems and ICT components, which are used in many different sectors of the Digital Single Market.

7. ACKNOWLEDGES the current developments at Union level to raise the level of cybersecurity of connected devices, particularly with regard to recent initiatives of the Commission to address in short-term cybersecurity aspects in relevant legal acts, for example acts under the New Legislative Framework (NLF), particularly Directive 2014/53/EU (Radio Equipment Directive). UNDERLINES the importance of assessing the need for horizontal legislation, also specifying the necessary conditions for the placement on the market, in the long-term to address all relevant aspects of cybersecurity of connected devices, such as availability, integrity and confidentiality. WELCOMES in this regard a discussion to explore the scope of such a legislation and its links with the cybersecurity certification framework as defined under the Cybersecurity Act (CSA), with the aim of raising the level of security within the Digital Single market.

8. STRESSES that cybersecurity requirements should be defined in line with the relevant Union legislation, including the CSA, the NLF, the Regulation on European Standardisation and a possible future horizontal legislation, to avoid ambiguity and fragmentation in legislation.

9. ACKNOWLEDGES the important role of all stakeholders, in particular of the manufacturers, to raise the level of cybersecurity of connected devices in the Digital Single Market, therefore CALLS for coordination and close cooperation with all relevant public and private stakeholders, also in view of a possible future horizontal legislation.

9a. WELCOMES the ongoing work led by ENISA to draft the first EU cybersecurity certification schemes, namely the proposed European Union Common Criteria and the proposed Cloud Service schemes. These schemes will be relevant foundations to certify connected devices.

10. EMPHASISES that any additional certification scheme for connected devices and related services that would be laid down in the Union Rolling Work Programme and defined under the CSA should specify how the applicable security requirements at the relevant assurance level should be met on the basis of specific European and internationally recognised standards, regardless of the sector in which the product is to be used, and which test specifications, certificates etc. are to be applied.

11. ACKNOWLEDGES that the certification of connected devices would require relevant norms, standards or technical specifications for cybersecurity evaluations under the CSA. Therefore, EMPHASISES the need to establish cybersecurity norms, standards or technical specifications for connected devices and RECOMMENDS strengthening efforts undertaken by European Standards Organisations in this matter. At the same time, NOTES the ETSI EN 303 645 cybersecurity standard for consumer IoT devices as an important step in this direction.

12. INVITES the Commission to consider a request for candidate cybersecurity certification schemes for connected devices and related services based on the Union Rolling Work Programme currently being developed taking utmost account of the horizontal European cybersecurity certification schemes currently being developed. On a voluntary basis such a scheme will enable the manufacturers of such products to promote products with the assessed assurance level.

13. INVITES a discussion on how the goal of cybersecurity could be anchored in a future horizontal legislation that covers cybersecurity risks related to connected devices, and at the same time NOTES the need to consider the adaptation of essential requirements of the respective NLF Directives, where appropriate.

14. ENCOURAGES the Commission to also assess, where necessary, complementary sector-specific regulations that should define which level of cybersecurity should be met by the connected device to ensure that specific security and privacy requirements are put in place for such devices with higher security risks.

15. STRESSES the need to improve the quality of life and well-being of the European citizens and foster the trust in the Digital Single Market. The security and privacy of our societies are essential to preserve our core values of the Union. Thus, STRESSES the need to build upon the framework provided by the CSA to harmonise security requirements, according to different assurance levels, across all sectors of the NLF in order to avoid fragmentation and multiple checks of identical requirements and offers a level playing field across the European Union for competition and innovation.

16. INVITES the Commission, the EU Agency for Cybersecurity (ENISA), the Telecommunication Conformity Assessment and Market Surveillance Committee, and the European Cybersecurity Certification Group (ECCG) to actively participate in this initiative of strengthening the Digital Single Market and enhancing the trust in ICT products, services and processes for connected devices by ensuring privacy and cybersecurity and to facilitate the increased global competitiveness of the Union's IoT industry through ensuring the highest standards of resilience, safety and security.

17. HIGHLIGHTS in this context the need to support SMEs as an essential building block of the European cybersecurity ecosystem, and ENCOURAGES the SMEs to take part in all public consultations launched as well as in standardisation activities to take into account their valuable and important contribution in the way of making cybersecurity a reachable target as well as a competitive advantage on the European market.

18. NOTES that the obligation to ensure cybersecurity and privacy throughout a product's entire life cycle and across its supply chain could have a positive impact on the technology sector's environmental footprint by leading manufacturers towards smart and sustainable development and production processes and thereby decreasing the amount of electronic waste related to the disposal of connected devices.