EUROPEAN COMMISSION

Brussels, 3.8.2018
C(2018) 5350 final

Mr Michael MÜLLER
President of the Bundesrat
Leipziger Straße 3 - 4
D – 10117 BERLIN

Dear President,

The Commission would like to thank the Bundesrat for its Opinion on the proposal for a Regulation of the European Parliament and of the Council on [the European Union Agency for Network and Information Security] ENISA, the "EU Cybersecurity Agency" and repealing Regulation (EU) 526/2013, and on Information and Communication Technology security certification ("Cybersecurity Act") {COM(2017) 477 final}.

This proposal forms part of a broader package of ambitious measures designed to increase the overall cybersecurity of the Union by addressing what the Commission considers to be key priorities in this field: reinforced resilience, the creation of a single market for cybersecurity, effective European Union cyber deterrence and strengthened international cooperation.

The proposal for a strong, permanent and focused mandate of the European Union Agency for Network and Information Security builds on the main achievements of the Agency in the field of cooperation, support to capacity building and policy development and implementation at Union level and the requirements of European Union law, in particular the important tasks attributed to the European Union Agency for Network and Information Security by the Directive on Security of Networks and Information Systems[1]*. At the same time, it entrusts the European Union Agency for Network and Information Security with some new responsibilities in the to-be-established European Union cybersecurity certification framework, which forms integral part of the proposal.*

Strengthening the users' trust in the digital single market by increasing the transparency of the security properties of Information and Communication Technology products and series is at the heart of the Commission's proposed Union-wide certification framework. The new rules will ensure that European Union companies undergo one single certification process per product/service to obtain a cybersecurity certificate which

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union; OJ L 194, 19.7.2016, p. 1–30.

would be valid throughout the European Union. The voluntary approach will avoid extra burdens for European companies and ensure the needed flexibility in such a fast-moving field as that of Information and Communication Technologies.

The Commission is pleased that the Bundesrat shares the view that action at Union level is required to strengthen European capacities and cooperation in cybersecurity and that it supports the need for a European framework for cybersecurity certification. It also welcomes the Bundesrat's support for the overarching objectives of the proposal.

The Commission takes seriously the concerns expressed by the Bundesrat as regards the respect of the principles of subsidiarity and proportionality. It stresses that the interdependencies between networks and information systems are such that individual actions of Member States very often cannot face the threats, manage the risks and possible impacts of cyber incidents. Increasing the cyber resilience of the Union and reinforcing the users' trust in the Digital Single Market, which are the main objectives of the proposal, are issues of common interest of the Union.

The scope of the proposal remains confined to the functioning of the internal market, from which issues related to the national security, which remain exclusive competence of the Member States, are explicitly and upfront excluded. The Commission also emphasises that its proposal builds on the existing successful national and European experiences and competences, which will continue to play a fundamental role in the future.

The Bundesrat's Opinion has been made available to the Commission's representatives in the ongoing negotiations with the co-legislators, the European Parliament and the Council, and will inform these discussions. On the basis of the constructive discussions that are taking places with the co-legislators, the Commission remains hopeful that an agreement will be reached before the end of its current mandate in 2019.

In response to the more technical comments in the Opinion the Commission would like to refer to the attached Annex.

The Commission hopes that the clarifications provided in this reply address the issues raised by the Bundesrat and looks forward to continuing the political dialogue in the future.

Yours faithfully,

Elżbieta Bieńkowska

Member of the Commission

Annex

The Commission has carefully considered each of the issues raised by the Bundesrat in its Opinion and is pleased to offer the following clarifications.

As regards the concerns raised on the role attributed to the European Union Agency for Network and Information Security in relation to a possible lowering of national security standards, as recalled in the Opinion, the mandate of the European Union Agency for Network and Information Security is established without prejudice to the competences of the Member States regarding cybersecurity, and in any case, without prejudice to activities concerning public security, defence, national security and the activities of the state in areas of criminal law [Article 3(3) of the proposal]. In addition, the proposed cybersecurity certification framework does not contradict or question current practices or lower existing standards. Member States retain their right to regulate the level of security for a given product/service category which is not covered by a European scheme.

In relation to the revised mandate of the European Union Agency for Network and Information Security, in particular in the area of operational cooperation, the proposal allows the Agency to support the work of Member States and European Union institutions towards achieving collective resilience of the Union. More specifically, the tasks conferred upon the Agency in relation to the operational cooperation build on the provisions of the Directive on Security of Networks and Information Systems[2]. It entrusts the European Union Agency for Network and Information Securitywith the secretariat of the Computer Security Incident Response Teams Network, the provisions of the current Regulation concerning the European Union Agency for Network and Information Security[3], which already foresees the possibility for Member States and European Union institutions to request support in the event of a breach of security with significant impact, and the new policy initiatives at Union level. These tasks do not replace or overlap with the roles and responsibilities of Member States. On the contrary, they aim to support Member States in improving their capacity to prevent, detect and respond to incidents and to contribute to operational cooperation at Union level in particular as far as cross-border issues are concerned.

With regard to Member States' role in the certification framework, these will play a fundamental role via the European Cybersecurity Certification Group established in the proposal, by proposing to the Commission the preparation of the certification schemes, assisting the European Union Agency for Network and Information Security in the preparation and review of the certification schemes and via the examination procedure on the implementing acts that will establish each scheme. In addition, while the

---

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union; OJ L 194, 19.7.2016, p. 1–30.

[3] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004; OJ L 165, 18.6.2013, p. 41–58.

European Union Agency for Network and Information Securitywill have a role in preparing the certification schemes, the operation of the schemes, including the testing of products in laboratories, issuing certificates, monitoring and enforcement will remain the competence of Member States and will be carried out at a national level.

The Commission has also made a careful assessment on whether to have in place a mandatory or a voluntary certification system. While the proposal establishes clear rules for the set-up of certification schemes as well as a system of penalties in case of non-compliance, due to the wide range of possible sectors and Information and Communication Technologies products and services involved, it was decided to keep the use of certification schemes voluntary. However, should Union law otherwise require it for specific sectors or categories of products, it will be possible to mandate the use of the schemes established under the framework.

With regard to the concerns expressed on the insufficient coordination with other European Union policies, the proposal stresses that the proposed certification framework is without prejudice to existing specific provisions regarding voluntary or mandatory certification in other Union acts, such as the Radio Equipment Directive[4], the Regulation on electronic identification and trust services[5] or the General Data Protection Regulation[6].

In the Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" {JOIN(2017) 450 final} the Commission also highlighted that work is under way to analyse the specific issues concerning liability for the digital technologies and what the possible implications for the current legal framework are. In this effort, the Commission will also take into account the results of the evaluation of the Directive on liability for defective products[7] and of the Machinery Directive[8].

[4] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC; OJ L 153, 22.5.2014, p. 62–106.

[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; OJ L 257, 28.8.2014, p. 73–114.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; OJ L 119, 4.5.2016, p. 1–88.

[7] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products; OJ L 210, 7.8.1985, p. 29–33.

[8] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast); OJ L 157, 9.6.2006, p. 24–86.