EU Regulation

CYBERSECURITY – PART 2: CERTIFICATION

cep**PolicyBrief** No. 2018-16

cep Centrum für Europäische Politik

KEY ISSUES

Objective of the Regulation: The Commission wants to set up a European cybersecurity certification scheme in order to increase confidence in products and services in the information and communication technology (ICT) sector.

Affected parties: All consumers and companies, particularly in the ICT sector, the EU cybersecurity agency ENISA, national supervisory authorities, conformity assessment and accreditation bodies.

Pro: (1) EU-wide cybersecurity certification rules may stimulate the market for cyber-secure ICT products and -services.

Contra: (1) It is questionable whether the Commission and ENISA have the know-how to determine which ICT products and -services sensibly require an ECCS.

(2) Member States should be compulsorily involved in the preparation of ECCSs.

(3) The EU legislator is not permitted to adopt any cybersecurity rules relating to the national security of Member States. It should therefore be clarified that Member States are permitted to require a higher level of protection in this regard and to maintain NCCSs.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Proposal COM(2017) 477 of 4 October 2017 for a **Regulation** of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and **on Information and Communication Technology cybersecurity certification**

Brief Summary

► **Context and objectives**

– According to the Commission, increasing digitisation and connectivity in many areas of society are leading to a rise in cybersecurity risks and attacks (Recitals 2 and 3).

– In view of these challenges, the Commission therefore wants to (Recital 5)
  - increase the capabilities of Member States and businesses in combating cyber attacks,
  - improve cooperation between Member States and EU institutions and
  - improve confidence in the digital single market with more transparency about the level of security provided by information and communication technology (ICT).

– This will essentially be achieved by (Explanatory Memorandum p. 3 and 6, Recital 11)
  - reform of the EU cybersecurity agency "ENISA" (see cep**PolicyBrief**) and
  - the certification of the cybersecurity of ICT (this cep**PolicyBrief**).

► **Current status of cybersecurity certification in the EU**

– Certification of the cybersecurity of information and communication technology (ICT) in the EU is currently based on various agreements and on initiatives by individual Member States (Explanatory Memorandum p. 8 and 9):
  - An international agreement regulates recognition of the "Common Criteria (CC) for Information Technology Security Evaluation", which has been signed by 13 Member States; the CC constitute an international standard for IT security evaluation.
  - The "SOG-IS" agreement, concluded by twelve EU countries plus Norway, regulates reciprocal recognition of certificates for a limited number of products such as digital signatures.
  - UK, France and Germany have set up national initiatives on ICT certification.

► **Future set of rules on cybersecurity certification in the EU**

– According to the Commission, the various agreements and initiatives are resulting in a fragmentation of the market. Companies often have to go through several certification procedures which increases their costs and the administrative burden. (Explanatory Memorandum, p. 9)

– With the Regulation, the Commission wants to establish a "European framework" for certifying the cybersecurity of ICT products and -services (Explanatory Memorandum, p. 9 and 10, Recitals 52 and 53).

Authors: Philipp Eckhardt and Dr. Anja Hoffmann, LL.M. Eur. | eckhardt@cep.eu

– The core element of the framework is made up of individual "European cybersecurity certification schemes" (hereinafter: ECCS) developed by ENISA for specific ICT products and -services or groups thereof. The ECCS that are developed will constitute the relevant set of rules on certification for the relevant ICT products and -services or groups thereof. (Explanatory Memorandum p. 9, 10, Recitals 52 and 53, Art. 44 (1))
– The term "ICT products and -services" also includes processes and systems as well as combinations of these elements (Art. 2 No. 11, Recital 47).
– Prior to preparing each ECCS, ENISA consults all "relevant" stakeholders, and the new cybersecurity certification group that is to be established (hereinafter: Group), which is made up of the representatives of the national certification authorities and chaired by the Commission (Art. 44 (2), Art. 53).
– The Commission engages ENISA to prepare an ECCS. "Member States" or the Group may request the Commission to engage ENISA with the preparation. (Art. 44 (1))
– The Commission adopts the prepared ECCS by way of implementing acts (Art. 44 (3) and (4)).

► **Security objectives, minimum content and assurance levels of the various ECCSs**

– The Regulation establishes "security objectives" (Art. 45) and "minimum content" (Art. 47 (1)).
– The following "security objectives" apply to all ECCS (Art. 45):
  - data is protected against accidental or unauthorised storage, processing or disclosure,
  - only authorised persons, programmes or machines can access the data, services or functions of the ICT products and -services,
  - ICT products and -services are provided with up to date software without known vulnerabilities.
– When preparing a specific ECCS, the following minimum content must be determined (Art. 47 (1), Explanatory Memorandum p. 10 and 12):
  - the cybersecurity requirements, e.g. by reference to European or international standards,
  - the types and categories of ICT products and -services that are covered by the ECCS and
  - the assurance levels, i.e. level of security that is to be guaranteed by the ECCS.
– ECCS-certified ICT products and services may be classified into three assurance levels - basic, substantial or high (Art. 46).

► **Cybersecurity certification based on an ECCS**

– Natural or legal persons that want to have their ICT products or services certified based on a specific ECCS, must request certification from the "conformity assessment body" and provide it with all the necessary information (Art. 48 (5), Recital 58).
– The conformity assessment body assesses whether the ICT products or -services meet the requirements of the relevant ECCS and issues the cybersecurity certificate (Art. 2 No. 14 and 15, Art. 48 (3)).
– "National accreditation bodies", appointed by the Member States, issue the conformity assessment bodies with the accreditation to carry out their work. Accreditation is issued for five years but may be extended. (Art. 51 in conjunction with Art. 4 (1) Regulation (EC) No. 765/2008)
– Certificates that have been issued are "presumed" to comply with the requirements of the specific ECCS (Art. 48 (1)). Certificates do not, however, "guarantee" compliance with cybersecurity requirements (Recital 47).
– Certificates are issued for a maximum of three years but may be renewed (Art. 48 (6)).
– Certificates that have been issued must be recognised in all Member States (Art. 48 (7)).
– Certification is voluntary, unless otherwise specified under EU law (Art. 48 (2)).

► **Role of Member States and the national supervisory authorities**

– Every Member State appoints a "national certification supervisory authority" which inter alia (Art. 50 (1) and (6))
  –checks certificates that have been issued by the conformity assessment bodies,
  –supervises the activities of conformity assessment bodies and
  –cooperates with other national supervisory authorities or other public authorities.
– The national supervisory authorities must notify the Commission of the conformity assessment body responsible for each specific ECCS (Art. 52).
– The work of ENISA is "without prejudice" to the competences of the Member States regarding cybersecurity. This applies "in any case" to activities concerning national and public security, defence and criminal law matters. (Art. 3 (3))

► **National and industrial cybersecurity certification schemes**

– Where an existing national cybersecurity certification scheme ("NCCS") also applies to ICT products and -services that are the subject of an ECCS, the NCCS becomes invalid as from the date specified in this regard by the Commission in its implementing act relating to the ECCS (Art. 49 (1)).
– Member States are not permitted to introduce any new NCCS for ICT products and -services that are covered by an ECCS. Certificates issued under the NCCS remain valid until their expiry date. (Art. 49 (2) and (3))
– Private certification schemes, inter alia operated by industry, are outside the scope of the Regulation. Responsible bodies can however request the Commission to approve their scheme as an ECCS. (Recital 53)

Statement on Subsidiarity by the Commission

There are major interdependencies between networks and information systems. These interdependencies mean that individual actors alone are no match for the threats to cybersecurity and cannot manage them in isolation. EU measures are therefore necessary.

Policy Context

In 2016, the Commission submitted a Communication on strengthening Europe's cyber resilience [COM(2016) 410] in which it considered framework rules on certifying the security of ICT products and services. In 2016, the Council also urged the Commission to take action.

Legislative Procedure

4 October 2017	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Directorates General:	DG Communications Networks, Content & Technology (leading)
Committees of the European Parliament:	Industry, Technology and Energy (leading), Rapporteur: Angelika Niebler (EPP Group, Germany)
Federal Ministries:	Federal Ministry for Home Affairs (leading)
Committees of the German Bundestag:	Home Affairs (leading)
Decision-making mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

Formalities

Competence:	Art. 114 AEUV (Internal market);
Type of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

There are two reasons why investment in cybersecurity remains low. Firstly, most consumers are not in a position to assess how "cybersecure" certain products and services actually are. Their willingness to pay for products and services that claim to be secure is therefore limited. Consequently, suppliers are also reluctant to invest. As a result of this informational asymmetry, the level of cybersecurity remains low ("market for lemons"). Secondly, many consumers avoid investment in cybersecurity because the individual loss, in the event of what is seen as an unlikely security incident, appears to be small. In taking this decision, however, they fail to take account of the negative consequences that their security incident may have for third parties (failure to internalise external effects) and they profit from investment made by third parties (free-riding).

EU-wide rules on cybersecurity certification may alleviate the problem of information asymmetries and **stimulate the market for cyber-secure ICT products and -services.** For this to happen, certification has to be seen as credible by consumers. The problem of the failure to internalise external effects and the free-riding problem will continue to exist however. Certification also tends to make products and services more expensive. This counteracts the positive effects. **The** planned **cybersecurity certification schemes – ECCS – will result in a significant increase in the power of ENISA and the EU Commission.** Only these authorities ultimately decide on the introduction and design of ECCS. **It is** however **questionable whether the Commission and ENISA have the** required **know-how to determine which ICT products and -services sensibly require an ECCS and how this should be designed**. In particular, in the case of ENISA, it is also doubtful whether it has the necessary staff for the preparation of ECCS (see cep**PolicyBrief** on ENISA reform). Also lacking is a precise definition of what qualifies as "ICT products and -services" under the Regulation – perhaps also processes for developing them –, and of the extent to which ECCSs cover cases involving the national security of Member States.

The fact that, in future, **companies will be able to have** their **ICT products and -services certified in a Member State and the certificates will then receive EU-wide recognition** ("one-stop-shop")**, reduces their costs but carries the risk that,** for the purposes of certification, **they will select the Member State in which it is easiest to obtain certification.** This in turn leads to the risk of lax examination of cybersecurity requirements and results in less secure ICT products and -services. This may be remedied by way of a monitoring procedure among the national supervisory authorities or by ENISA.

The fact that certification itself basically remains voluntary is appropriate. Only in highly sensitive areas of application could mandatory certification be justifiable. In areas of minor risks to third parties regarding cybersecurity, certification seems to be an unnecessary and expensive barrier to market entry and ultimately impedes innovation.

Legal Assessment

Legal Competency

The rules on certification are covered by the internal market competence (Art. 114 TFEU). Although harmonisation is not governed solely by the Regulation, because the details are contained in the ECCSs, legal acts can also be based on Art. 114 where they simply confer competence upon the Commission to effect harmonisation by way of implementing measures (CJEU, Case C-66/04, para. 51). Due to the technical complexity of the material, **the EU legislator** can also enlist the help of ENISA as a body responsible for contributing to harmonisation of the ECCS (cf. CJEU, Case C-217/04, para. 44 et seq.). It **cannot,** however, **adopt any cybersecurity rules relating to the national security of Member States.** This is the sole responsibility of the Member States (Art. 4 (2), sentence 3 TEU). It should therefore be made clear that the Member States are permitted to require a higher level of protection in this regard and, where required, to maintain (complementary) NCCS.

Subsidiarity.

The EU framework for certification is compatible with the principle of subsidiarity. Although there is already a recognition agreement for national certificates between 12 Member States, in the form of the "SOG-IS MRA", in practice this is only used for the certification of products which require high assurance levels. Comprehensive harmonisation for products with low assurance levels or for ICT services can only be achieved by way of a separate EU framework.

In principle, implementation of EU law is the task of Member States. The EU legislator can however empower the Commission to establish ECCS by way of an implementing decision where "uniform conditions for implementation" are required (Art. 291 (2) TFEU). **The Commission should however establish the ECCS not in implementing acts** (Art. 291 TFEU) **but in delegated acts** (Art. 290 TFEU), because it is supplementing the Regulation by way of the ECCS and not "implementing" it in the narrower sense. This would also strengthen their democratic legitimacy.

This is not prevented by the fact that important details of the certification such as products and technical requirements are only established in the ECCSs. Although the EU legislator is obliged to regulate all essential aspects itself, only provisions implementing the fundamental guidelines of EU policy are considered to be "essential" (CJEU Case C-240/90, para. 37). The fundamental guidelines of certification - objectives, components and effects of the ECCSs - are however laid down by the Regulation.

Proportionality with respect to Member States

The Regulation encroaches upon the power of the Member States to regulate cybersecurity in their own country. The invalidity of NCCS and the obligation to recognise all ECCSs, may result in a reduction in the level of protection in the Member States. **In order to achieve a high level of technical security** (Art. 114 (3) TFEU) **and avoid a failure of ECCS** in the comitology procedure (see Recital 65) or objections to the delegated act, **Member States and business should be compulsorily involved in their preparation** rather than just "consulted". **There should also be** express **clarification of the fact that Member States are permitted to attach stricter** (national) **requirements to the use of ICT products and -services, insofar as this is necessary for the protection of important national interests** – including those which go beyond the narrow field of "national security" – such as public safety, defence or criminal law (Art. 3 (3)).

Impact on German Law

The law on the Federal Office for Information Security (BSIG) and the BSI Certification and Recognition Regulation, in particular, will have to be amended.

Conclusion

EU-wide rules on cybersecurity certification may stimulate the market for cyber-secure ICT products and -services. It is questionable whether the Commission and ENISA have the know-how to determine which ICT products and -services sensibly require an ECCS. The EU legislator cannot adopt any cybersecurity rules relating to the national security of Member States. It should therefore be made clear that the Member States are permitted to require a higher level of protection in this regard and to maintain NCCS. The Commission should establish the ECCS in delegated acts rather than implementing acts. In order to achieve a high level of technical security and avoid a failure of ECCS, Member States should be compulsorily involved in their preparation There should also be clarification of the fact that Member States are permitted to attach stricter requirements to the use of ICT products and -services, insofar as this is necessary for the protection of important national interests.