Europe *EU*

The New EU Cybersecurity Act: one step closer to a more secure future

Introduction

The proliferation of connected devices across industry sectors has led to the emergence of a significant and distinct threat to many types of organisations. However, a majority of European companies continue to underestimate just how exposed they are to cyber risk[9]. This lack of awareness translates into low investment in Internet of Things (IoT) cybersecurity and limited legal risk management.

Against this backdrop, the European Commission (the "Commission") has been developing and adopting the EU Cybersecurity Strategy, with the European Network and Information Security Agency (ENISA), created in 2004, making an active contribution to policy[10]. Initially established for a period of five years, ENISA's mandate has been progressively extended[11], revised and modernised.

At launch, ENISA's mission was principally to provide advice and assistance and enhance cooperation between EU bodies and Member States in the field of cybersecurity. Over the 2013-2016 period, ENISA's performance, governance and organisational structure were evaluated by the Commission[12]. Based inter alia on its findings and on the consultation of various stakeholders, the Commission concluded that ENISA's mandate was not sufficient and adopted a new cybersecurity package on 13 September 2017[13]. It proposed a new Regulation providing ENISA with a strengthened and permanent mandate and creating an EU-wide cybersecurity certification framework[14].

Enisa's strong mandate

The cybersecurity ecosystem is changing all the time with new challenges emerging from the transformed cyber threat landscape. To ensure ENISA can fit into and respond to this new environment, the Cybersecurity Act strengthened its powers to improve coordination and cooperation in cybersecurity across the EU and granted it a permanent status from 27 June 2019.[15] The financial and human resources allocated to ENISA have also been increased.

From now on, ENISA will act as the EU's cybersecurity expert, providing advice and expertise to Member States, private stakeholders, European institutions and policymakers,[16] and helping Member States to implement the Directive on the Security of Network and Information Systems.[17]

Its new objectives are to raise cybersecurity standards across the EU by (i) assisting Member States and EU institutions, bodies, offices and agencies in developing and implementing EU general cybersecurity policy,[18] (ii) supporting capacity building and preparedness,[19] (iii) supporting operational cooperation and coordination among the various actors,[20] and (iv) promoting the use of cybersecurity certification.[21] To that end, ENISA will perform various analyses of emerging technologies, cyber threats and incidents. It will also provide advice and guidance, and develop guidelines and best practices.[22]

ENISA works with competent authorities to issue warnings targeted at manufacturers and providers, and requiring them to improve the security of their information and communications technology

9 European Commission, Commission Staff Working Document, Impact assessment accompanying the document proposal 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, Part 1/6, p. 41.

10 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

11 ENISA's mandate was last extended until 19 June 2020 by Regulation (EU) No 526/2013.

12 Study on the Evaluation of the European Union Agency for Network and Information Security, Final Report.

13 European Commission, Press release, State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks, September 19, 2017.

14 Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification.

15 Cybersecurity Act, Recital 16.

16 Cybersecurity Act, Article 3.

17 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 (NIS Directive)

18 Cybersecurity Act, Article 5.

19 Cybersecurity Act, Article 6.

20 Cybersecurity Act, Article 7.

21 Cybersecurity Act, Article 8.

22 Cybersecurity Act, Article 9.

(ICT) products and services where these do not meet cybersecurity standards.[23] More generally, it assists Member States and national authorities to prevent and improve responsiveness to cyber threats and incidents.

EU cybersecurity certification framework

The Commission wants connected devices and IoT technologies to incorporate security features in the early stages of development. It is also important that customers should be able to identify the level of security of the products or services they purchase.[24] This is particularly true for devices – like connected products and services in the healthcare sector – that require a high level of security. To achieve this goal, the Cybersecurity Act creates the first EU-wide cybersecurity certification framework.

At the moment, security certification schemes exist in some sectors where cybersecurity is a critical consideration, such as automated cars and electronic medical devices.[25] But when such certification exists, it is only recognised in the Member State concerned.[26] This means that companies have to certify their ICT products in several Member States if they plan to market them across the EU, which is costly for companies and inefficient for the Digital Single Market (DSM).

For that reason, the Cybersecurity Act adopts a uniform approach to prevent "certification shopping".[27] Specifically, it establishes "a European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognised and used in all Member States".[28]

ENISA will assist with designing candidate cybersecurity certification schemes that will then be adopted by the Commission.[29] Every certification scheme will specify an assurance level ("basic", "substantial", or "high").[30] Conformity self-assessment is possible for products and services presenting a low risk with a "basic" assurance level. In such cases, manufacturers and providers issue a statement of conformity under their sole responsibility.[31]

ENISA will also launch a European Cybersecurity Certification website.[32] This will contain certification schemes, certificates and statements of conformity, and should build trust among end-users.

Each European cybersecurity certification scheme must include inter alia the "maximum period of validity of European cybersecurity certificates issued under the scheme."[33] ENISA will evaluate each adopted European certificate scheme at least every five years.[34]

Recourse to European cybersecurity certification is voluntary, unless otherwise specified by EU or Member State law.[35]

Any existing national certification scheme covered by the new European certification scheme will cease to be effective.[36] Any existing certificate issued under a national certification scheme and covered by the new European certification scheme remains valid until its expiry date.[37]

Comment

The Cybersecurity Act further strengthens EU cybersecurity policy, enabling manufacturers of ICT products to demonstrate – across the EU – that their products are secure. It should also improve access to information and build trust among the end-users of certified connected products.

23 Cybersecurity Act, Recital 51.
24 Cybersecurity Act, Recitals 7 and 10.
25 Cybersecurity Act, Recital 65.
26 Cybersecurity Act, Recital 67.
27 Cybersecurity Act, Recital 70.
28 Cybersecurity Act, Recital 69.
29 Cybersecurity Act, Articles 8 and 48.
30 Cybersecurity Act, Article 52.
31 Cybersecurity Act, Article 53.
32 Cybersecurity Act, Article 50.
33 Cybersecurity Act, Article 54.
34 Cybersecurity Act, Article 49.
35 Cybersecurity Act, Article 56.
37 Cybersecurity Act, Article 57.

The success of the new certification framework will depend on how readily it can be adapted to deal with constantly evolving cyber threats, market developments and industry specifics. The Commission will play a significant role here by regularly assessing "the efficiency and use of the adopted European cybersecurity certification schemes".

Also, because certification is not mandatory, the framework's objectives will be met only if ICT manufacturers and providers make full use of it. Last, it remains to be seen how this new Regulation will work with existing regulations, including the General Data Protection Regulation (GDPR) and the NIS Directive.

Charles-Henri Caron
Counsel, Paris
T +33 1 53 67 47 47
charles-henri.caron@hoganlovells.com

Anne-Laure Morise
Knowledge Lawyer, Paris
T +33 1 53 67 38 75
anne-laure.judlin@hoganlovells.com