EUROPE LAUNCHES A NEW CYBERSECURITY AGENCY WITH REGULATORY AUTHORITY

Date: 19 September 2017

Brussels Regulatory Alert

By: Alessandro Di Mario, Ignasi Guardans

BACKGROUND

On 13 September 2017 the European Commission ("Commission" or "EC") published a set of initiatives strengthening the EU cybersecurity strategy, mainly including:

- A proposal for a "Cybersecurity Act", consisting of a new regulation **on ENISA and on Information and Communication Technology cybersecurity certification** along with an **Annex**;
- A Staff Working Document including an Executive Summary of the Regulation's **Impact Assessment**;
- A Communication regarding the effective implementation of the already approved Network and Information Security Directive (NIS Directive).

Through this set of measures, the Commission aims to increase cybersecurity preparedness, resilience and harmonisation, while avoiding implementation contradictions and regulatory fragmentation across the EU.

This is the last big step in a formal Strategy that included other provisions in the digital and cybersecurity policy area, specifically the NIS Directive, the eIDAS Regulation and the Radio Equipment Directive. A previous comment on the NIS matters can be found here.

This alert will focus on the proposed new Cybersecurity Act Regulation (the "Regulation").

CONTENT SUMMARY

The Regulation can be divided into two blocks:

- **The reorganisation and reinforcement of ENISA (title II)**

ENISA is the European Union Agency for Network and Information Security, based in Heraklion, Crete, Greece. It was established by Regulation 460/2004/EC, while Regulation 526/2013/EU extended its mandate until 2020 and already strengthened its role. The objective of ENISA was to improve network and information security in the European Union by assisting the Union institutions, bodies, offices in developing policies in the field; in implementing policies necessary to meet the legal and regulatory requirements; in enhancing their capability to prevent, detect and respond to security incidents.

From the outset, the Cybersecurity Act Regulation grants a clearer and more permanent mandate to ENISA and reinforces its role, turning it into the "EU Cybersecurity Agency". It also outlines a new scope of its mandate

adding new areas, in particular those regarding the consistency in the implementation of the NIS Directive, the upcoming Cybersecurity Blueprint for cyber crisis cooperation, and functions related to security certification in Information and Communications Technology ("ICT").

Operationally, the new Agency will work both with the public and the private sector. On the one side, it will contribute to the improvement of public authorities' capabilities and advising them in R&D, including in the context of the contractual public-private partnership on cybersecurity. It will also facilitate cooperation among Member States in dealing with cybersecurity emergencies and reinforce the existing preventive operational capabilities. On the other side, the Agency will share best practices on cybersecurity and will assume the main role in the EU policy regulatory developments regarding the ICT cybersecurity certification area.

- **The establishment of a Cybersecurity Certification Framework for ICT products and services (Title III)**

At the time of this proposal, there are several mutual recognition agreements and several other initiatives among Member States regarding the matter of cybersecurity certification of ICT products and services, which relate also to a larger, international framework, the so-called "Common Criteria" for Information technology Evaluation. The EC describes this fragmented reality as "patchy", and having identified its serious costs and its impact in market fragmentation, it wants to establish a real new European scheme. A new **Cybersecurity Certification Framework** (the "Framework") will be based on European Cybersecurity Certification Schemes which will set out the scope of cybersecurity certifications through specific features, for instance the identification of categories of products and services covered, the specification of cybersecurity requirements and the level of assurance they are intended to guarantee (basic, substantial or high).

Such schemes will be prepared by ENISA with the advice of the European Cybersecurity Certification Group—consisting of national certification supervisory authorities of all Member States—and adopted by the Commission. Once the scheme is adopted, manufacturers and providers will be able to submit an application for certificate their ICT products and services to a conformity assessment body of their choice. These will be third-party independent bodies established under national law and accredited by an accreditation body after assessment of compliance of certain specified requirements.

The creation of this Framework should provide companies with a single procedure for cybersecurity certification, reducing costs, facilitating cross-border operations and avoiding fragmentation. Moreover, it is intended to increase cybersecurity assurance for ICT products and services of pivotal sectors (transport, energy, health, automotive, finance among others) and raise consumers' trust.

Monitoring, supervisory and enforcement tasks will not be centralized at EU level: they will lie with the Member States, each one of which will have to create a certification supervisory authority assuming all compliance obligations, together with investigative capabilities on such compliance.

NEXT STEPS

There should be general political consensus behind the new proposal, so the Cybersecurity Act Regulation is expected to smoothly follow the ordinary legislative procedure, with amendments to be discussed and proposed separately by the Parliament and the Council. However, it is too early to anticipate if there will be challenges to try

to reduce or adjust the new "red tape" imposed by the Cybersecurity Act; and whether all Member States will easily accept both what the Regulation prevents them to do (separate certification schemes), as well as the burdens imposed upon them regarding the creation of new assessment and certification bodies and authorities.

