March 2019

IS THE EU ANSWERING A CALL FOR MORE CYBERSECURITY IN LIGHT OF THE DEVELOPMENTS AROUND 5G?

Nicola Benz/Cornelia Mattig

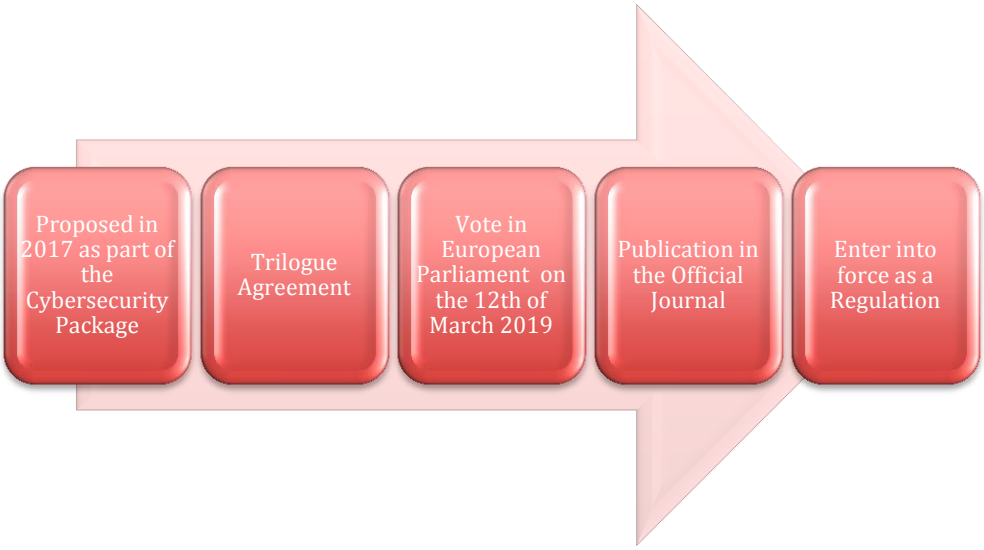
Media have increasingly covered cybersecurity issues in the last couple of months addressing in particular the USA's race against China to build the fifth generation of wireless technology (5G technology) and its security aspects. Although there is a widespread worry of increased cyber intrusions once the 5G technology is widely available there is also a huge possibility for new internet-based services. This is because 5G is designed to provide users with a much faster wireless connection allowing for new innovations in different areas (e.g. Internet of Things) to become a more integrated part of our daily life.

In fact, nowadays cybersecurity already affects many sectors that are dependent on digital technology such as finance, health, energy and transport. With the introduction of 5G, the scope of affected services will only increase. Already today many business models are based on a constant dependency of the internet and functioning information systems (e.g. cloud computing, machine-to-machine communications or e-payments). The disruption of such services is considered a cybersecurity incident. They can be caused by attacks, natural disasters or unintentional mistakes. Therefore, there is a need to limit such incidents to a minimum to ensure the constant availability of such services.

Even though 5G offers many possibilities in this area we also need to ensure that the network is secure for such innovations. Against this backdrop, the EU has adopted the 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 ("Cybersecurity Act") as part of its Cybersecurity Package. Besides the strengthened security measures, the new Cybersecurity Act will align different parameters and technical requirements relating to the construction and implementation of IT services and devices.

Where are we now? When do we have to consider EU-wide technical requirements?

Although the European Parliament passed the new Cybersecurity Act this month, this does not mean it enters into force immediately. The Cybersecurity Act was proposed in 2017 alongside other initiatives to strengthen cybersecurity such as the Network and Information Security Directive and a stronger focus on security measures in the General Data Protection Regulations (GDPR). As with these other regulatory measures, there will be a transition period. For the Cybersecurity Act, the transition period is likely to last for a similar time period meaning for 2 years.



What is this new Cybersecurity Act all about?

The EU institutions proposed this Cybersecurity Act with the argument that security and resilience are not sufficiently built into technical products, services or processes. Considering the technical developments in the area of IoT, cloud computing, machine learning and artificial intelligence, the advancement of more secure devices, services and processes, the proposal of a Cybersecurity Act did not encounter much resistance. Although the Cybersecurity Act is addressing security concerns it may create an entry barrier for start-ups or smaller firms active in these fields.

The Cybersecurity Act in its current form is split into two parts.

1. Certification Framework

The new Cybersecurity Act will introduce cybersecurity certification scheme for certain services and processes with regard to Information Communications Technology (ICT) products and the products as such including hardware and software elements of networks and information systems. The creation of a European Cybersecurity Certification Framework

for ICT products and services will allow for products and services to be certified once for the whole of the EU and no longer require several authorisation processes.

The European Union Agency for Network (ENISA) will be tasked with preparing such schemes for specific product categories in cooperation with the European Cybersecurity Certification Group. These schemes will then be adopted by the Commission. This means that the Cybersecurity Act does not set out a scheme but defines the legal basis for ENISA to draw up product-specific schemes. Each of those schemes will have its own scope and can include specific conditions for recognition in third countries such as Switzerland. The certification schemes may specify three sets of assurance level on different aspects including resilience to accidental or malicious data loss or alterations. The level will then define the applicable set of rules. Although ENISA will prepare the schemes of the conformity assessments, they will be carried out by national bodies or in certain cases allow for self-assessment.

This new Cybersecurity Certification Framework highlights the focus of the Cybersecurity Act to promote security by design instead of security by default, which intends to strengthen the trust of users.

2. Permanent Mandate for ENISA

The new Cybersecurity Act also provides ENISA with a permanent mandate and new tasks to support member states, EU institutions and other stakeholders regarding these issues. The Agency will have more resources and play a crucial role in cooperation and coordination at the EU and Member State level to address cybersecurity threats as well as incidents. It will also offer a single point of access for more guidance to address security concerns.

What does this mean for my business?

There are positive and negative aspects of the new Cybersecurity Certification Framework. It is certainly positive to

- strengthen trust and confidence around new innovative technology; and
- create one set of rules for the whole of the EU so that companies do not have to get certifications from several member states.

At the same time, such regulation may hinder innovation by increasing barriers with regard to new products and services for start-ups and young companies.

What does this mean for my business in Switzerland?

ENISA can cooperate with third countries such as Switzerland and/ or international organisations to address global cybersecurity issues. Article 39 of the Cybersecurity Act expressly provides that the ENISA may, subject to prior approval by the Commission, establish working arrangements with third countries and/ or international organisations. ENISA will also be open to participation of third countries if they have entered into Agreements with the EU to that effect. In the case of Switzerland such cooperation seems unlikely in the near future without first entering into a framework agreement with the EU.

In any case, businesses should keep up to date with these developments and adapt their security compliance programs accordingly. FRORIEP will help you stay informed to keep track of the latest developments while accompanying you on the way to ensure compliance with new regulatory requirements.

WHO IS FRORIEP?

Founded in Zurich in 1966, Froriep is one of the leading law firms in Switzerland, with offices in Zurich, Geneva and Zug, as well as foreign offices in both London and Madrid, serving clients seeking Swiss law advice.

We have grown a domestic and international client base ranging from large international corporations to private clients. Our unique, truly integrated, international structure mirrors our strong cross-border focus. We value and promote continuity and strong client relationships. Our teams are tailor-made, assembled from every practice area and across our network of offices.

Many of our lawyers are recognised as leaders in their practice areas, and our clients benefit from our in-depth knowledge and the rich diversity of talents, languages and cultures that makes our lawyers particularly versatile and adaptive.

ZURICH
Bellerivestrasse 201
CH-8034 Zurich
Tel. +41 44 386 60 00
Fax +41 44 383 60 50
zurich@froriep.ch

GENEVA
4 Rue Charles-Bonnet
CH-1211 Geneva 12
Tel. +41 22 839 63 00
Fax +41 22 347 71 59
geneva@froriep.ch

ZUG
Grafenaustrasse 5
CH-6302 Zug
Tel. +41 41 710 60 00
Fax +41 41 710 60 01
zug@froriep.ch

LONDON
17 Godliman Street
GB-London EC4V 5BD
Tel. +44 20 7236 6000
Fax +44 20 7248 0209
london@froriep.ch

MADRID
Antonio Maura 10
ES-28014 Madrid
Tel. +34 91 523 77 90
Fax +34 91 531 36 62
madrid@froriep.ch