GDPR - How it may clear up the digital market

Anett Mádi-Nátor, Cyber Services Plc.

Setting the scene – Cybercrime costs 2017-2021

Cybercrime cost estimates have risen from $400 billion in early 2015 to $6 trillion by 2021.

By 2020 the world will need to cyber-defend 50 times more data than it does today.

Cybersecurity Ventures projects $1 trillion will be spent globally on cybersecurity from 2017 to 2021.

Business values – Impact

CEOs will exit 30% of their CMOs for not mustering the blended skill set of design and analytics.

In 2017, CIOs will take the plunge and become business leaders to address external and personal risk.

Business heads will see doubled attrition rates as CEOs dig in and appoint leaders with both digital and customer competencies.

Transitional roles like chief data officer, chief digital officer, and chief customer officer will continue to get reintegrated into traditional roles.

In 2017, the basic fabric of trust is at stake as CEOs grapple with how to defend against escalating, dynamic security and privacy risk.

Source: FORRESTER.COM

Why is that so?

WHY?

THE REASON:

CybeServices

Data is a new (natural) resource

Data is the new oil

DATA has become a new asset

DATA has become a (natural) resource

Data is the TARGET

There is no such thing as „for free” - private data is monetized

Data is monetized – private individuals pay with their personal data sets for „free” services.

Consider such data as a kind of virtual currency – How should it be protected? How about regulating its use? How about restricting data overuse?

Another angle – Cyber warfare

- GLOBSEC Bratislava Forum (17-19 May 2018), a global policy making platform for security
- There is growing emphasis laid on a new area that is relation between technology any security. The role and consequences of cyberwar are in a constant grow.
- Christopher Painter's thoughts in summary (coordinator for cyber issues to the Obama Administration): Consequently we see that there is practically an ongoing status of cyber conflicts. There are attacks and infiltrations. There is a need for creating the code or treaty of cyber warfare, just like similar ones exist for physical warfare.
- (The picture on the left is only for illustration, taken from a Hungarian edition of Euronews.)

CybeServices

A set of answers

Actual cyberspace related initiatives, strategies, and legislations in EU

- Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace of 7 February 2013;

- Concerning measures for a high common level of security of network and information systems (NIS) across the Union of 6 July 2016 (EU 2016/1148);

- 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 (GDPR - EU 2016/679);

- Electronic identification and trust services for electronic transactions in the internal market (eIDAS – EU No 910/2014);

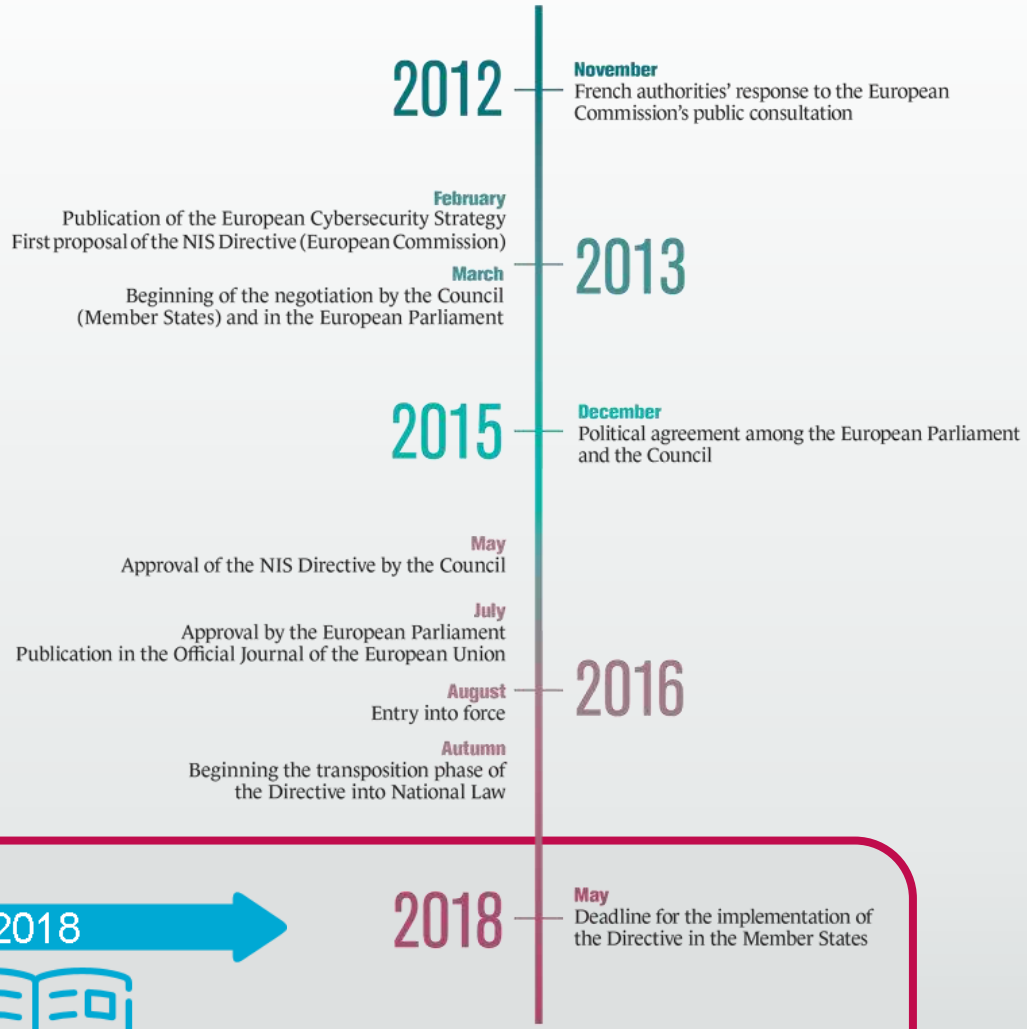
- A Digital Single Market Strategy for Europe of May 2015;

- Contractual Public Private Partnership on Cybersecurity – European Cyber Security Organisation (ECSO), 2016.

Timeline – NIS and GDPR

The **GDPR** must be binding and directly applicable to all Member States.

Definitions of **NIS Directive** will be applied to the member states' national legislations, so it must be applied in the Hungarian legal system too. The complete implementation of the Directive will begin in 2018 May.



Motivation

- Creating a **digital safe haven** for EU and 3rd country digital service providers and EU private individuals (users, in a different term customers in a B to C business environment)
- Creating a virtual border protection package to protect digital data within
- Providing business opportunity to better quality digital services – to create (EU) added value in the globalised digital economy

How?

- By enforcing better digital services through enforcing GDPR **security by design** and **privacy by design** fundaments
- By **financially severely punishing** those digital service providers who do not comply and suffer a significant data set compromise
- By **creating a common legislation in a federated environment** (in EU)
- By supporting the **digital single market** initiative
- By setting the legal and technological basis for a next generation EU IT environment – the **digital autonomy** initiative

Thank you for your attention
Riga 2018