European Regulation on Cybersecurity and Data Protection

Peter Fatelnig
Minister Counsellor for Digital Economy Policy
Delegation of the European Union to the United States of America

US-German Standards Panel - April 10, 2018
The current EU Playbook

2018 reform of EU data protection rules

Regulation on the Free Flow of Non-personal Data

European Cyber Security Package

Public Private Partnership for Cyber Security

Privacy Shield
Building EU Resilience to cyber attacks

- **Reformed ENISA**
- **EU cybersecurity Certification Framework**

Creating effective EU cyber deterrence

- Identifying malicious actors
- Stepping up the law enforcement response
- Stepping up public-private cooperation against cybercrime
- Stepping up political and diplomatic response
- Building cybersecurity deterrence through the Member States’ defence capabilities

Strengthening international cooperation on cybersecurity

- Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
- Advancing EU cyber dialogues
- Modernising export controls, including for critical cyber-surveillance technologies
- Continue rights-based capacity building model
- Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence

Cybersecurity Act

Communication

- Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund
- Cybersecurity competence network with a European Cybersecurity Research and Competence Centre
- Building strong EU cyber skills base, improving cyber hygiene and awareness

Cybersecurity Act

Communication

- Building EU Resilience to cyber attacks
- Creating effective EU cyber deterrence
- Strengthening international cooperation on cybersecurity

Cybersecurity Act

Communication

- Reformed ENISA
- EU cybersecurity Certification Framework

Creating effective EU cyber deterrence

- Identifying malicious actors
- Stepping up the law enforcement response
- Stepping up public-private cooperation against cybercrime
- Stepping up political and diplomatic response
- Building cybersecurity deterrence through the Member States’ defence capabilities

Strengthening international cooperation on cybersecurity

- Promoting global cyber stability and contributing to Europe’s strategic autonomy in cyberspace
- Advancing EU cyber dialogues
- Modernising export controls, including for critical cyber-surveillance technologies
- Continue rights-based capacity building model
- Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence
ENISA - New Mandate & Objectives

- Be an independent centre of expertise
- Assist EU Institutions and MSs in policy development & implementation
- Support capacity building & preparedness
- Promote cooperation & coordination at Union level
- Promote high level of awareness of citizens & businesses
- Contribute to high Cybersecurity
- Increase cybersecurity capabilities at Union level to complement MSs action

Promote the use of certification & contribute to the cybersecurity certification framework
ICT cybersecurity certification

Our Proposals: A voluntary European cybersecurity certification framework...

...to enable the creation of individual EU certification schemes for ICT products and service.

...that are valid across the EU
How will the framework work in practice?

- European Commission requests ENISA to prepare a Candidate Scheme.
- ENISA prepares a candidate scheme.
- ENISA transmits the candidate scheme to the European Commission.
- European Commission adopts the candidate scheme.
- A European Cybersecurity Certification Scheme is established.
- European Cybersecurity Certification Group (MSs) advises ENISA or may propose the preparation of a scheme to the Commission.
Objectives of the Network Information Security Directive

- Increased national cybersecurity
- EU level cooperation
- Security & Notification

Boosting the overall cybersecurity in Europe