Package of initiatives on Cybersecurity

Presentation to Members of the IMCO Committee

Claire Bury
Deputy Director-General, DG CONNECT
Brussels, 12 October 2017
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

Cybersecurity Act
- NIS Directive Implementation

Communication
- Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund

Recommendation
- Cybersecurity competence network with a European Cybersecurity Research and Competence Centre
- Building strong EU cyber skills base, improving cyber hygiene and awareness

Stepping up public-private cooperation against cybercrime
- Stepping up political and diplomatic response
- Building cybersecurity deterrence through the Member States' defence capabilities
Ensuring the full implementation of NIS

- Put in place comprehensive and ambitious national strategies
- Ensure effective and adequately resourced national CSIRTs
- Ensure effectiveness of implementation and enforcement
- Align the national approaches on Operators of Essential
- Extend the scope of the NIS Directive to additional sectors, e.g. public administration
ENISA - New Mandate and objectives

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

Contribute to high Cybersecurity
Handling large scale Cybersecurity incidents

Blueprint - Cooperation at all levels

- **Technical**: Incident handling; Monitoring and continuous analysis of threats and risk
- **Operational**: Preparing decision-making; Coordinate the management of the cybersecurity crisis; Assess the impact at EU level
- **Political**: Management of both cyber and non-cyber aspects of the crisis including Cybersecurity Emergency Response Fund

- Allow Member States to seek help at the EU level during or following a major incident.
- Complement existing crisis management mechanisms at EU level.
- Rapid response capability in the interests of solidarity.
- Draw on national expertise along the lines of the EU Civil Protection Mechanism.
European Cybersecurity Research and Competence network & Centre
ICT cybersecurity certification: Our proposal

A voluntary European cybersecurity certification framework...

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

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

In a nutshell: EC proposes & decides, Group advices (and may propose), ENISA prepares schemes
Proposal for a Regulation on the Free Flow of Non-personal Data

Presentation to Members of the IMCO Committee

Claire Bury
Deputy Director-General, DG CONNECT
Brussels, 12 October 2017
Proposal for a Regulation

- **Adopted** by the Commission on 13 September 2017 (SoTEU).

- **Essence**: Member States may no longer require businesses and citizens to store or process data within their territory.

- **Core problem**: Obstacles to data mobility in the EU.

- Important element of the **DSM strategy** since the outset.
Evidence gathering process by the European Commission:

- 2 public consultations: platforms, online intermediaries, data, cloud computing and the collaborative economy in 2015; building a European data economy in 2017;
- 4 dedicated studies and study workshops;
- 3 structured dialogue meetings with MSs and numerous bilateral discussions;
- Stakeholder engagement / workshops;
- 2 impact assessments.
Obstacles to data mobility

- **Data localisation requirements** by Member States' public authorities;

- **Vendor lock-in** practices by cloud service providers;

- **Legal uncertainty** leading to caution on the market regarding cross-border data storage and processing;

- **Lack of trust** due to security risks and concerns about the cross-border availability of data for regulatory purposes.
Unlocking cross-border data storage and processing for EU business

• Creating legal certainty for cross-border storing and processing of data within the EU;

• No multiplication of IT systems for EU companies (SMEs) active in different Member States;

• Enabling innovative cross-border data ecosystems in Europe;

• A competitive EU single market for secure, reliable and affordable cloud services (avoiding vendor lock-in).
The proposed Regulation:

- **Principles-based**, not detailed (Better Regulation):
  - The free flow of non-personal data principle
  - The principle of data availability for regulatory control purposes
  - Actions to make sure cloud service providers and users develop self-regulatory codes of conduct for easier switching of provider and/or porting data back to in-house servers
  - Governance by single points of contact per Member State, forming an expert group.
Single EU Data Space

EU data flows: the rules

- Personal data
- Protection of citizens
- Privacy

- Non-personal data
- Opportunities for business
- A competitive data market

GDPR
FREE FLOW OF NON-PERSONAL DATA

7
Free movement of data is essential for the European Data Economy

- Data and data flows "feed" technological innovation (IoT, AI, blockchain, fintech, smart mobility, e-health)
- Enabling free flow of data in the EU is estimated to grow the European Data Economy with an additional 4% of the GDP by 2020