WORKSHOP ON RISK ASSESSMENT AND SECURITY MEASURES FOR PERSONAL DATA PROCESSING

ENISA - Rome, February 08, 2018

Towards an effective approach to risk assessment in data processing

Alessandro Mantelero

Associate Professor of Private Law - Polytechnic University of Turin

I. THE SCENARIO

- ✓ **Risk analysis and risk management as essential elements of data protection regulations**
- ✓ **Two different paradigms: the risk-based approach and the rights-based approach**
- ✓ **The rights-based approach in the EU data protection regulations**

- ✓ **Directive 95/46/EC (security of processing, prior checking, organizational measures)**

- ✓ **National implementations:**
  - **Difficulties concerning the adoption of technical provisions**
  - **Weak enforcement**
  - **Costs and lack of support**
  - **Focus of risk assessment models on data security**
  - **Formal compliance**

II. THE GDPR AND ITS FUTURE IMPLEMENTATION(S)

- ✓ **From legitimacy of data processing and data subject's self-determination to controllers' accountability and risk management (Articles 5, 24, 32, 35-36)**
- ✓ **Shortcomings:**
  - **Self-assessment**
  - **Link with the purposes of data processing**
  - **Underestimation of non-security-focused risks**
  - **Underestimation of the collective dimension of data protection**
  - **Lack of awareness/competence among SMEs (e.g. Italian DPC 2003)**

III. TOWARDS AN EFFECTIVE APPROACH TO RISK ASSESSMENT IN DATA PROCESSING

- ✓ **Going beyond the administrative/formal approach**
- ✓ **Providing adequate and operative support to SMEs (ENISA, Handbook on Security, 2017)**
- ✓ **Focusing on risk theory and risk management models**
- ✓ **Focusing on data uses**

✓ **Recognising the role played by research projects**

"The research community and competent EU bodies, in close collaboration with regulators (e.g. Data Protection Authorities), should propose and put forward methodologies that combine security risk management and risk management of personal data" (ENISA, Handbook on Security of Personal Data Processing, 2017)

✓ **Adopting a broader approach**

- **Council of Europe: Guidelines on Big Data**
- **The PESIA model (H2020 Virt-EU project): risk awareness as a competitive advantage**

Alessandro Mantelero @mantelero

PLTRG - Polito Law & Technology Research Group

- Data protection
- HRI & Cyborgs
- Product liability
- ICT Law
- Data ethics

@PolitoLTRG