

Deploying ENISA methodology

Practical use cases

Georgia Panagopoulou

MSc Computer Engineer & Informatics

HDPA ICT Auditor

gpanagopoulou at dpa.gr

Security of Personal Data Processing Event - Athens, October 8th



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

The **goal**: practical demonstration and application of the methodological steps

Apply the steps of the methodology in order to define/request/estimate appropriate security measures.



Inspire, facilitate SMEs - Even with no “data protection expert”, no DPO



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



The **means**: SMEs cases simulation

 use case

- specific **personal data processing operation**
- specific **assumptions on the data processing environment**
- assumptions on overall context of processing.**



The use cases focus **ONLY** on security measures

- No legal analysis
- No assessment of overall GDPR compliance



The **way**: various SME sectors – different risk levels and types of personal data

- ❑ Context of the processing
 - ❑ *experience of data controller's cases, notifying and requesting authorizations from DPAs.*

- ❑ Specific SME sectors - cases “simulation”

- ❑ Idea to include: “Typical” SMEs with personal data processing of different risk levels and types of personal data.
 - ❑ E.g Health & insurance sector, travel & accommodation services, commercial shops and e-shops, education ...



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



The **outcome**: SME sectors – “horizontal” processings

- Mapping of processing operations per sector
- Some processing operations considered as “horizontal” - relevant to all vertical sectors
- Examples:
 - ❑ Personal data processing of employees for human resources purposes
 - ❑ Customer and potential customers, suppliers personal data processing, for different purposes like order and delivery of goods, marketing/advertising, supply of services and goods
 - ❑ The purpose of safety and security, achieved via tools like access control, Closed Circuit Television System (CCTV)




ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



The **challenges** of the exercise

- Evaluation of Impact on Confidentiality, Integrity, Availability
 - Under certain circumstances the overall impact higher than the proposed one
 - Difficulty to define scenarios, suggestions on what to consider
 - Risk assessment for each processing operation
-  Controls applied per system/per organization



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



The **conclusions**

- One-size fits all approach not viable
- Each processing operation to be reviewed separately
- Context and environment of the processing matter
- Data controllers should comprehend their processing operations and then evaluate the level of risk and deploy the appropriate security measures.
- Role of an appropriately qualified Data Protection Officer (DPO)
- GDPR Certifications
- Sectorial Codes of Conducts, DPIA templates



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr



Thank you for your attention



ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

