CONFERENCE ON PERSONAL DATA BREACHES

Supporting data controllers in assessing the risk of a personal data breach
Organized by EDPS-ENISA, Brussels 4 April 2019

IT Policy, Dina Kampouraki
PERSONAL DATA BREACHES

• GDPR Articles 33 & 34; (+ Police Directive Articles 30 & 31)
• EDPR, Regulation 2018/1725 Articles 34 & 35 (+ Articles 92 & 93)
• EDPS Guidelines on Personal Data Breach Notification for EU Institutions and Bodies
• Online notification tools, specific form provided
• Security (encryption) of transmission and processing of data breach notifications
• DPO Network, case studies and various raising awareness activities (trainings, workshops, etc)
ACTIONS FOR COMPLIANCE TO PERSONAL DATA BREACHES

Prepare to avoid and/or handle a breach
- Internal procedures
- Invest in Security
- ISMS
- Resilience
- Awareness Training
- Review 3rd party Contracts
- Prepare a Risk Matrix
- Breach register

Act in case of a Breach
- Correct Identification
- Incident response team
- Effective communication
- DPO involved
- **Assessment of Risk**
- Notification to SA
- Communication to persons

Review and fix things
- Lessons learned
- Corrective actions
- Review Procedures, etc
- Awareness Training
RISK BASED APPROACH: ASSESSING IMPACT OF A BREACH

• Case by case basis: **objective assessment**

• Likelihood and severity to the rights and freedoms of the individuals by reference to nature, scope context and purposes of the processing
  
  • **Nature, Volume, Sensitivity, Context**

• DPIA and its role to assessing a risk

• 12 Different Practical examples are provided into the EDPS Guidelines with indications to Risk and High Risk
OBSERVED DIFFICULTIES

• Correct identification of a Personal Data Breach
  • examples where notifications with no risk were submitted or were risk was immediately mitigated

• Internal Communication problems

• Assessment of Risk (different approaches observed)

• Timely respond and notify the Supervisory Authority (within 72 hours)
THE WAY FORWARD

• Building our experience:
  More concrete examples are needed

• EDPB working on that direction and
  EDPS is actively participating
THANK YOU!

For more information
www.edps.europa.eu
@EU_EDPS
edps@edps.europa.eu