‘MOSTLY HARMLESS’

DATA BREACH NOTIFICATION UNDER REGULATION (EU) 1725/2018

DPO Meeting, Frankfurt 17 May 2019

IT Policy, Xabier Lareo
DATA BREACH NOTIFICATION – STATE OF PLAY

- The EDPS received a total of 31 notifications from all sorts of EU Institutions and bodies (EUI).
- 3 personal data breach notifications concern incidents where special categories of data are involved (health data (2) and political opinions (1)).
- 6 notifications were received after the 72 hours threshold. In one case the processor delayed significantly to inform the processor in due time.
- The controller decided to notify the data subjects in 10 cases.
TYPE OF DBN

![Bar Chart]

- **Complete Notifications**: 22
- **Notification in Phases**: 9
NUMBER OF DBN PER CONTROLLER SIZE

- Big: 71%
- Medium: 19%
- Small: 10%
NUMBER OF AFFECTED DATA SUBJECTS

- Less than 10: 13
- Between 10 and 99: 6
- Between 100 and 999: 10
- More than 1000: 2
ROOT CAUSE

- Human Error: 78%
- Technical Bug Functionality: 19%
- External Attacker: 3%

24
6
1
LESSONS TO BE LEARNED

• The risk of a human error causing a data breach can be avoided or mitigated.

• The aim of providing data controllers 72 hours to notify is not to ‘solve’ the data breach.

• The data breaches distribution does not correlate with the size of the institution. Data breach prevention is for all.

• Communication between data controllers and processors must be agile. This requires both contractual and operational safeguards.

• Risk assessments of the impact on data subjects privacy must be formal, objective and documented.
OBSERVED DIFFICULTIES

• Timely respond and notify the Supervisory Authority (within 72 hours)
  - Internal Communication problems delayed the process
  - Lack of decision on the incident

• Correct identification of a Personal Data Breach
  - Notifications with assessment of no risk
  - Notifications were risk are completely avoided

• Lack of training and awareness

• Assessment of Risk (different approaches observed) in line with DPO skills
MEETING THE 72 DEADLINE

• The hours of a Saturday or Sunday count as much as the hours of a Monday.

• There is nothing wrong in using a phased notification.

• Personal data breaches are security incidents ▶ Incident response plan.
  • Who will do what
  • Who should be informed
  • How to get in contact with the external and internal stakeholders
  • Templates
  • Awareness raising exercises

• Adequate communication policy and channels with data processors.

• Do not hesitate to contact the EDPS if in doubt. We will help you.
RISK BASED APROACH: ASSESSING IMPACT OF A BREACH

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

• Likelihood and impact to the rights and freedoms of the individuals by taking into account for 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 NO Risk, Risk and High Risk
THANK YOU!

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