PATRICIA Exercise

Personal Data Breach Awareness Campaign

NewsFlash on Personal Data Breaches

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

27 November 2024
DPO Meeting Luxemburg

DB Management Survey

Personal data breach awareness initiative

Reminder: Initiative design

DESIGN

A Questionnaire was designed in *EU Survey* with the aim to provide a way of **self assessment** of the internal procedures and practices. We identified ten personal data breach capabilities.

AIM

- We wanted to **engage** the controller to **reflect** on the personal data breach management process as implemented in the organization
- We used a **key metrics** approach to support the self assessment

EXPECTED OUTCOME

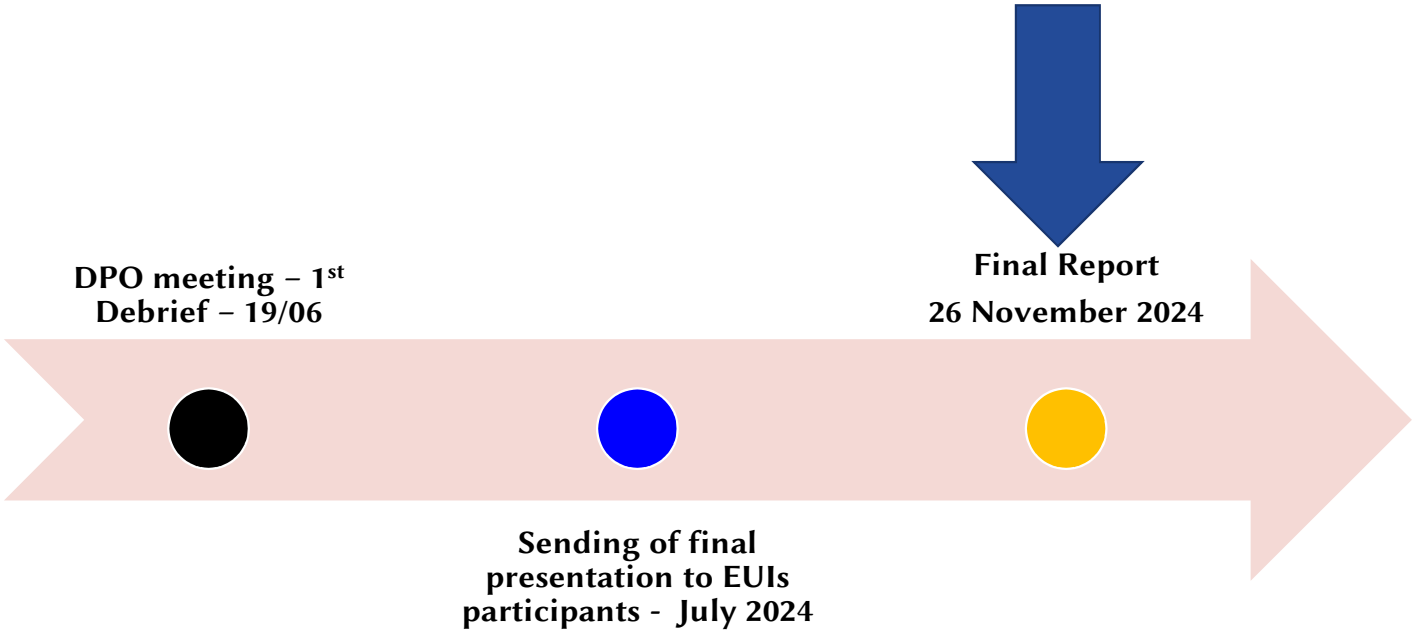
Through these lenses it helped the EDPS to open a free discussion with the EUIs on best practices in a more **dynamic** way.

FINAL OUTPUT

A report with

- **8 key findings** and associated recommendations
- An initial **roadmap** of actions for the following years

Data Breach Management survey



3 main conclusions

1. Controllers, through their DPOs, should ensure data protection awareness, including on the topic of personal data breach, of their staff.
2. Controllers do not always allocate sufficient resources to endorse compliance within the organisation's business processes and supporting tools and systems.
3. The EUIBAs' risk culture is underdeveloped, mostly due to the lack of an approved risk management framework, which recognises the risks to fundamental rights and freedoms of individuals as part of the overall business risks. They should be treated with the same risk-minded approach as for any kind of risks (financial, reputation or operational). Corollary, there is an acknowledged lack of knowledge on how to perform personal data breach risk assessment.

2025 Ambitions

- Launch the first Personal Data Breach Bulletin with use cases, link to informational resources.
- Renew the exercise with voluntary and designated controllers (in accordance to specific criteria);
- Improve the assessment toolkit with possible development of an automatic tool.
- Share the exercise methodology and toolkit
- Use the format of the exercise to other data protections areas (e.g., DPIA).

PATRICIA

Personal data breach awareness In cybersecurity incident handling

PATRICIA cyber-exercise

- Pilot on **3rd October 2024** at EDPS Premises
- **Table top exercise**
- 1 scenario with 3 incidents and then discussion

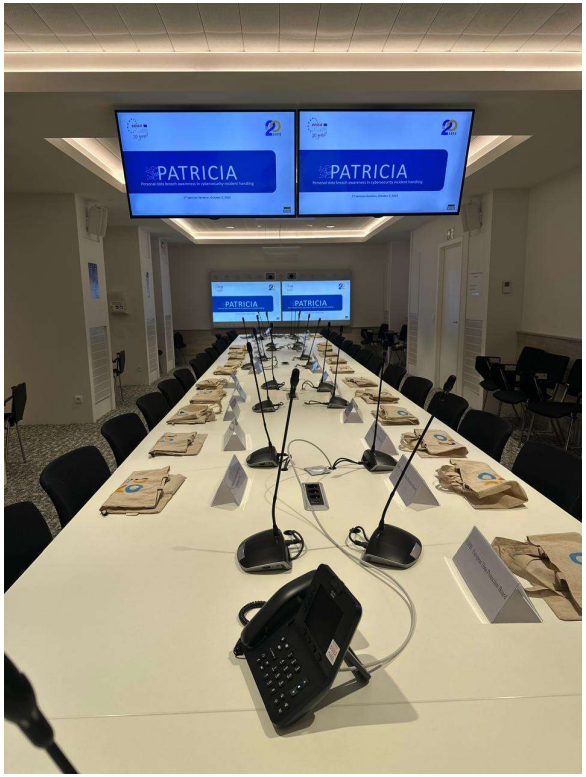
- **Aim:** to **raise awareness** of personal data breach management among employees of EUIBAs, especially IT personnel who would be involved in a cybersecurity incident and would need to collaborate with other roles in the EUIBA, to effectively manage a personal data breach

IT Managers

Information Security Officers

Data Protection Officers

- **6 Teams**



PATRICIA - Findings

Common understanding and coordination in personal data breach management needs to be advanced

- Internal committees
- Regular meetings
- Communication channels

Internal processes need to be updated

- Include new roles interacting with data breach processes, e.g. LCO role from Cybersecurity Regulation
- Harmonize internal reporting forms

There is need to further raise internal awareness

- IT teams to become more aware of controllership cases
- Develop a culture of shared responsibility to facilitate contacts and sharing of information

Training across disciplines is necessary

- Data protection
- Cybersecurity
- Technological elements

PATRICIA – Next steps

- **Receive comments from participants on the draft report (sent 26 November 2024) and finalise the report early 2025.**
- **Consider concrete proposals for actions.**
- **Propose a second iteration on Q2 2025 in the EDPS/ENISA strategic plan.**

Data Breaches Newsflash

in short, tips and tricks

News

New feature in the Data Breach Notification form

→ Inclusion of a question covering Art.21(1) of the Cybersecurity Regulation

→ Webform and Word document

D.18·Notification·of·Security·Incident·to·Cert-EU·in·accordance·with·Regulation·2023/2841·Art.21(1):·¶

YES·☐·NO☐¶

(If·the·data·breach·also·qualifies·to·be·a·significant·incident·in·accordance·with·the·Regulation·2023/2841·Art.·21(1),·then·reply·'Yes'.·You·must·then·inform·Cert-EU·separately)¶

News

CERT-EU threat alerts and security advisories - a source of information for supporting proactive data protection actions, learning about the risk landscape, ...

→ on the CERT-EU website (https://cert.europa.eu/publications/security-advisories/2024)

→ by email (ask you LSO/LISO)

News

Data breach notifications **statistical insights** for 2024:

→ TOTAL: 99

→ Top 3 root causes:

- Human error: 40
- External attack: 26
- Technical bug: 21

2004
2024
EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority