11 December 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

EDPS CAMPAIGN ON RAISING AWARENESS OF PERSONAL DATA BREACHES

A Comprehensive Initiative to Strengthen Compliance on personal data breach management

EDPS CAMPAIGN ON RAISING AWARENESS OF PERSONAL DATA BREACHES: A Comprehensive Initiative to Strengthen Compliance on Personal Data Breach Management

In 2024, the European Data Protection Supervisor (EDPS) launched a dedicated campaign to raise awareness of personal data breaches, one of 20 initiatives organised to mark the institution's 20th Anniversary. The campaign ran from March to October 2024, with participation from European Union Institutions, Agencies, and Bodies (EUIs) that had not previously notified the EDPS of any personal data breaches. Its goal was to enhance compliance with the legal obligations under Regulation 2018/1725 (referred to here as "the Regulation").

Objectives and Approach

The EDPS has steadily developed a robust supervisory approach towards EUIBAs that have to notify personal data breaches. The 2024 campaign built on this approach, taking into account the broader European cybersecurity landscape. Its objectives were to:

- **Enhance the EDPS' supervisory and advisory role** by engaging directly with EUIs.
- **Promote dynamic awareness** by encouraging EUIs to strengthen their personal data breach management processes.

The campaign followed a four-phase structure:

1. **Survey Questionnaire** – Measured the maturity of personal data breach management using a self-assessment tool.
2. **Data Sorting and Initial Analysis** – Assessed survey responses and created a Spider Chart for each EUI to visualise maturity levels.
3. **Active Cooperation** – Facilitated bilateral meetings to discuss findings and challenges.
4. **Final Report** – Summarised key observations, findings and recommendations.

Key Functional Pillars of Effective Personal Data Breach Management

Drawing on existing process building and improving frameworks, the EDPS identified three essential pillars for an effective personal data breach management process:

- **Foundation** – Establishing the core framework and resources for the process.
- **Operation** – Implementing the tools and procedures required to manage personal data breaches.
- **Improvement** – Reviewing, learning and improving processes over time.

Pillar I: Foundational capabilities	Pillar II: Operational capabilities	Pillar III: Improvement capabilities
(Q1) Process establishment/description (Art.34 and 35, 92 and 93, Art. 27 and 85)	**(Q3)** Notification process (Art.34 and 35, 92 and 93, Art.45(1)(d), recital 56)	**(Q10)** Continuous improvement (Art. 26(1), Art. 33(1)(d), Art. 27 and 85)
(Q2) Awareness and training (Art.45(1)(a))	**(Q5)** Data Breach documentation (Art.34.6, 92.4)	**(Q2)** Awareness and training (Art.45(1)(a))
(Q4) PDB detection (Art.33(1), recital 53)	**(Q7)** Data breach response (Art.33(1), recital 55)	**(Q6)** Processor control (Art. 29, Art.33(3), recital 51)
(Q6) Processor control (Art. 29, Art.33(3), recital 51)	**(Q8)** Data breach Reporting (Art.44(4) and (7), Art. 45(1)(d), recital 57)	**(Q8)** Data breach Reporting (Art.44(4) and (7), Art. 45(1)(d))
	(Q9) Data breach investigation/remediation (Art. 33(2), Art.45(1)(d) and (2))	**(Q9)** Data breach investigation/remediation (Art. 33(2), Art.45(1)(d) and (2))

Each of these pillars was linked to specific capabilities underpinned by provisions of the Regulation. The maturity self-assessment questionnaire was designed to measure these capabilities, with each question corresponding to a particular capability.

Key Findings and Challenges

The campaign analysis revealed eight key findings, drawn from survey responses and interviews with EUIs. These findings highlighted critical areas that require improvement in the management of personal data breaches. Key challenges were identified in the following areas:

- **DPO Profiles and Limitations**
  Data Protection Officers (DPOs) face constraints in terms of their role and capacity.
- **Process Establishment**
  Many EUIs lack a well-defined and mature personal breach management procedure.
- **Resource Allocation**
  Limited resources hinder the establishment and maintenance of a comprehensive personal breach management procedure.
- **Role of Processors**

Processors play a significant role, but their responsibilities and specific requirements often remain unclear.

- **Risk Management Development**

The absence of a formal risk management framework that addresses personal data risks poses a significant challenge.

- **Continuous Awareness and Training**

Ongoing training and awareness-building are essential to ensure that EUIs remain prepared for personal data breach incidents.

The analysis also measured the overall maturity of EUIs' personal breach management processes, offering a comparative view of their capabilities and areas for development.

Key Recommendations and Conclusions

The EDPS provided tailored recommendations to EUIs to address the above challenges. These recommendations aimed to enhance compliance, support organisational development, and improve the protection of data subjects' rights and freedoms. Additionally, the EDPS incorporated feedback from EUIs to ensure a more targeted and practical approach.

The campaign concluded with three key insights:

1. **Awareness and Training.**
   Controllers, with the support of their DPOs, should increase staff awareness on personal data breach risks.
2. **Resource Allocation**.
   More resources are needed to support compliance and maintain personal data breach management.
3. **Risk Culture**.
   EUIs need to establish a formal risk management framework to identify and mitigate personal data breach risks.

Future Directions

The EDPS proposed forward-looking measures to help EUIs address the identified challenges. These proposals aimed to further develop the personal breach management process, support the establishment of risk management frameworks, and ensure better allocation of resources for compliance efforts.

By fostering a culture of awareness, risk management, and continuous improvement, the EDPS campaign sought to strengthen the protection of personal data across EUIs. The campaign serves as a model for how supervisory authorities can actively support institutions in improving their compliance and in upholding the rights of data subjects.