12 December 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

"PATRICIA"

Personal dATa bReach awareness In Cybersecurity Incident hAndling

EDPS European Data Protection Supervisor
ENISA The European Union Agency for Cybersecurity

PATRICIA Exercise

Personal dATa bReach awareness In Cybersecurity Incident hAndling

On 3 October 2024, the European Union Agency for Cybersecurity (ENISA) and the European Data Protection Supervisor (EDPS) jointly organised a table-top exercise titled **"Personal dATa bReach awareness In Cybersecurity Incident hAndling" (PATRICIA)**. The event, hosted at the EDPS premises in Brussels, aimed to raise awareness among staff from European Union Institutions, Bodies, and Agencies (EUIs) on managing personal data breaches.

The PATRICIA exercise was developed as part of the strategic plan under the Memorandum of Understanding (MoU) between ENISA and the EDPS, which includes commitments to "design, develop, and deliver capacity-building and awareness-raising activities".

Participants and Structure

The exercise brought together 21 participants from six EUIs, including IT managers, Data Protection Officers (DPOs), and Security Officers (LISO, LCO), all of whom play key roles in managing cyber incidents involving personal data breaches. CERT-EU also participated as an observer, adding valuable insight from its experience with incident response.

The exercise spanned six hours and was divided into two sessions:

1. **Scenario-Based Incident Response** – Participants were introduced to the exercise scenario, which included three (3) incident "injects." Participants were organised into teams based on their respective EUIs and asked to respond to incident-related questions based on their internal processes. This approach encouraged reflection, discussion, and the exchange of best practices among teams.
2. **Debriefing and Lessons Learned** – The second session included a broader discussion on the participants' overall experience, feedback on possible improvements for future exercises, and a review of collaboration between different roles within EUIs.

Objectives of PATRICIA

The PATRICIA exercise was designed to achieve the following key objectives:

- **O1**: Test the readiness of EUIs to identify required actions and allocate responsibilities in the event of a personal data breach.
- **O2**: Raise awareness of the need to assess risks to data subjects' rights, particularly when cybersecurity incidents involve personal data.
- **O3**: Identify areas for improvement in communication and collaboration between IT teams, DPOs, and LISOs/Local Cybersecurity Officers.
- **O4**: Evaluate the efficiency of internal processes for personal data breach management, including the main steps and notification procedures.

After-Action Report and Recommendations

The exercise and subsequent discussions revealed important findings, which highlight areas for improvement in personal data breach management within EUIs.

Based on these findings, the EDPS and ENISA provided participants with a first draft for their review and comments outlining recommendations to improve existing processes and procedures. These recommendations aim to:

- **Foster a culture of shared responsibility** for breach management through greater involvement from senior management.
- **Harmonise roles and responsibilities** to ensure that stakeholders clearly understand their obligations.
- **Enhance communication and collaboration** between IT teams, DPOs, and LISOs.
- **Promote cross-disciplinary training** to build capacity across the various roles involved in personal data breach management.

Conclusions and Next Steps

The PATRICIA exercise was deemed a success by participants, who highlighted the value of identifying key gaps in internal processes, roles, and responsibilities. The exercise revealed the need to develop a common understanding of responsibilities across different stakeholder groups and emphasised the importance of fostering interdisciplinary cooperation and information sharing.

The positive feedback from participants underscored the value of the exercise, with many recommending that similar activities be conducted in the future. Participants suggested including more EUIs in future editions of PATRICIA and incorporating additional elements related to personal data breach management.

By addressing the issues identified and promoting shared responsibility, EUIs can improve their readiness to manage personal data breaches, reduce risks to data subjects, and comply more effectively with their obligations under Regulation (EU) 2018/1725.

This exercise serves as an example of how supervisory authorities like EDPS, in collaboration with ENISA, can support institutions in building capacity, fostering collaboration, and promoting continuous improvement in the management of personal data breaches.