EDPS

7 November 2025

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

"PATRICIA II"

Personal dATa bReach awareness In Cybersecurity Incident hAndling

Executive Summary

Executive Summary

On 5 June 2025, the European Data Protection Supervisor (EDPS) organised at the European Parliament's Info Hub premises a table-top exercise, named "Personal dATa bReach awareness In Cybersecurity Incident hAndling II" (PATRICIA II), aimed to raise awareness among European Union Institutions, Bodies and Agencies (EUIBAs) staff about personal data breach management in a cyber-attack context[1].

The EDPS would like to thank once again via this report, ENISA for their good collaboration in the first edition of the exercise and CERT EU for their collaboration and participation in this second edition.

Participants and Structure

The exercise brought together the IT managers, Data Protection Officers (DPOs) and Security Officers (LISO, LCO) from eight EUIBAs that would be responsible for collaborating and managing a cyber-incident resulting in a personal data breach. A total of thirty-six staff members from eight EUIBAs took part in the event, whereas CERT-EU joined as an observer.

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

1. **Scenario-Based Incident Response:** participants were introduced to the exercise scenario and to three (3) incidents ("injects"). They were divided into teams formed around their EUIBA of origin, and they were asked to respond to a series of questions per inject, according to their internal processes, in order to spark discussion. At the end of each incident, all questions were discussed, enabling also the exchange of ideas among teams.
2. **Debriefing and Lessons Learned:** At the end of each incident, all questions were discussed, enabling also the exchange of ideas among teams. The second session included a broader discussion on the overall satisfaction with the exercise, proposals for possible next editions of the exercise, as well as elements regarding collaboration of different roles within EUIBAs.

Goal and Objectives

The main goal of the PATRICIA II exercise was to **raise awareness of personal data breach management** among EUIBAs staff, 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**[2].

The Objectives set by PATRICIA II are the following:

Objective 1: **Identify the need to assess risk to data subjects**, as a result of a cybersecurity incident. This has to be done in addition to the risks for the organisation, since the risks for the data subject are often not the same that the ones for the organisation.
Objective 2: Identify expected actions or allocation of responsibilities to the different teams/roles involved in case of a personal data breach.

---

[1] *Raising awareness to controllers is one of EDPS tasks, according to article 57(c) of Regulation (EU) 2018/1725, (promote the awareness of controllers and processors of their obligations under this Regulation).*
[2] *According to articles 34 and 35 of Regulation (EU) 2018/1725 (EUDPR).*

Objective 3: Identify communications needs different actors such as IT teams, LISO/Local Cybersecurity Officer and DPO.
Objective 4: Evaluate if the organisation's internal processes on personal data breach management support the organisation on main steps and notifications outlines.

After-Action Report and Recommendations

EDPS provided participants with a first draft for their review and comments **After-Action Report** outlining recommendations to improve existing processes and procedures. These recommendations aim to:

- **Improve coordination and shared understanding:** Foster a common internal understanding of the interplay between roles and responsibilities in managing personal data breaches, including clear communication channels and protocols**.**
- **Enhance information exchange**: Develop a standardized glossary of key terms and concepts related to personal data breaches and cybersecurity incidents to ensure consistent understanding across all roles, and ensure all roles have a common understanding of security and personal data breach elements, including basic categories of measures and how they can be useful in the different contexts.
- **Streamline internal processes**: Harmonize existing processes and procedures related to breach management, including internal reporting forms and relevant tools or manuals, and develop links among them.
- **Promote interdisciplinary training and awareness**: Organize regular training sessions to enhance each role's knowledge on personal data breach management and bring together all stakeholders involved in data breach management, including IT security personnel, data protection officers, legal teams, and senior management.

Conclusions and Next Steps

The PATRICIA II exercise, organised by the EDPS, successfully achieved its goal of raising awareness and strengthening the understanding of personal data breach management among EUIBA staff, especially those working in IT and cybersecurity. For many participants, it was the first opportunity to discuss breach scenarios and internal procedures across different functions. This cross-departmental exchange proved essential in identifying gaps in the shared understanding of responsibilities and highlighted the need for a coordinated approach with clearly defined roles under all relevant legal frameworks.

Participant feedback was highly positive. The scenarios were considered realistic, and the discussions directly relevant to daily work. The event also underlined the importance of continuous training, improved information sharing, and learning from past incidents. In particular, one element that was highlighted by many participants is the need to take into consideration the risks for the individuals on top of the risks for the organisation when a security incident arises.

Looking ahead, the EDPS plans to adapt the exercise for larger, multi-DG organisations such as the European Parliament, Commission, and Council, where data protection structures are more complex. Future editions will feature new scenarios, invite additional EUIBAs that have not yet taken part, and integrate participant feedback to ensure even more realistic and challenging exercises, including the involvement of other controllers.