Raising Awareness in Personal Data Breaches

Awareness Campaign – Preliminary results

Technology & Privacy Unit

Dina Kampouraki – Head of Sector Systems Oversight and Technology Audits (SOTA)
• **Our Goal:** To evaluate the personal data breach management process implemented in the selected EUIs ([link](#)). An awareness activity around the data breach management process itself which promotes the exchange of ideas between the EUIs and the EDPS.

• **Participants:** EUIs that have never submitted a notification to EPDS (*1st Wave*)

• **Campaign structure:**
  - Step 1 - Questionnaire of 20 questions, split in 10 maturity self-assessment questions and 10 key-metrics questions
  - Step 2 – Individual bilateral meetings to go through the provided answers and more.
  - Step 3 - Summary of key findings - EDPS Bulletin dedicated on personal data breaches

• **Rate of participation:** on 20 EUIs, 17 answered the survey and 16 confirmed their participation
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

**OUTCOME**
Through these lenses it helped the EDPS to open a free discussion with the EUIs on best practices in a more dynamic way.
Bilateral Meetings arranged starting May 2024 (~ 1 hour)
We produced a power point presentation for each EUI containing:
- A review of the provided answers
- A spider chart with maturity assessment results
- Tailored questions
Exchanges of views on the exercise itself but also with regard to other topics which might not have been addressed during the bilateral
2 members of EDPS present during the online meeting
### Positive findings

<table>
<thead>
<tr>
<th>The DB Management Process is described via a <strong>policy or procedure</strong> with the inclusion of roles and responsibilities of each stakeholder involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>An extract of the <strong>established PDB register</strong> is made available internally in a simplified format as an awareness instrument.</td>
</tr>
<tr>
<td><strong>Reports are made to management</strong> systematically either on an ad-hoc basis or /and annually</td>
</tr>
<tr>
<td>Some <strong>interesting initiatives</strong> exist to ensure that the staff reports data breaches and that compliancy is materialised on tight budgets</td>
</tr>
</tbody>
</table>

### Current difficulties

<table>
<thead>
<tr>
<th>Difficulty to ensure that the process is efficient as there is a low number of personal data breaches (detected or declared) to gain experience from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of human, time and technical resources to capture and document the occurred or potential breach in a more automated way.</td>
</tr>
<tr>
<td><strong>Processor operational control is difficult</strong> to achieve due to lack of resources and to already standardised contractual provisions.</td>
</tr>
<tr>
<td><strong>The Institution’s risk appetite vs fundamental rights protection</strong> – these 2 dimensions are not treated equally as strategical goals</td>
</tr>
</tbody>
</table>
Campaign Survey : Timeline

- **DPO meeting – Debrief**
  - 19/06

- **Sending of final presentation to EUIs participants**
  - July 2024

- **Final Report**
  - October 2024
The EUIs welcome the campaign exercise:

1. the proposed follow-up to the initial questionnaire with a face-to-face meeting. This modus operandi is richer than just answering a survey.
2. the maturity self-assessment, while still high-level, gave the participants a compass that they can re-use (and improve/adapt to their organisation) to monitor their personal data breach process internally.
3. the exercise was considered as a wake-up call.
Campaign Survey: Future?

- Bring out the announced Data Breach Bulletin end of 2024 (as Xmas gift)
- Repeat the exercise in 2025 with other EUIs, to be selected or on a voluntary basis (Do you want to volunteer?)

YOUR PARTICIPATION MATTERS
&
YOU MADE IT A REALLY INTERESTING CAMPAIGN
EUROPEAN DATA PROTECTION SUPERVISOR
The EU’s independent data protection authority