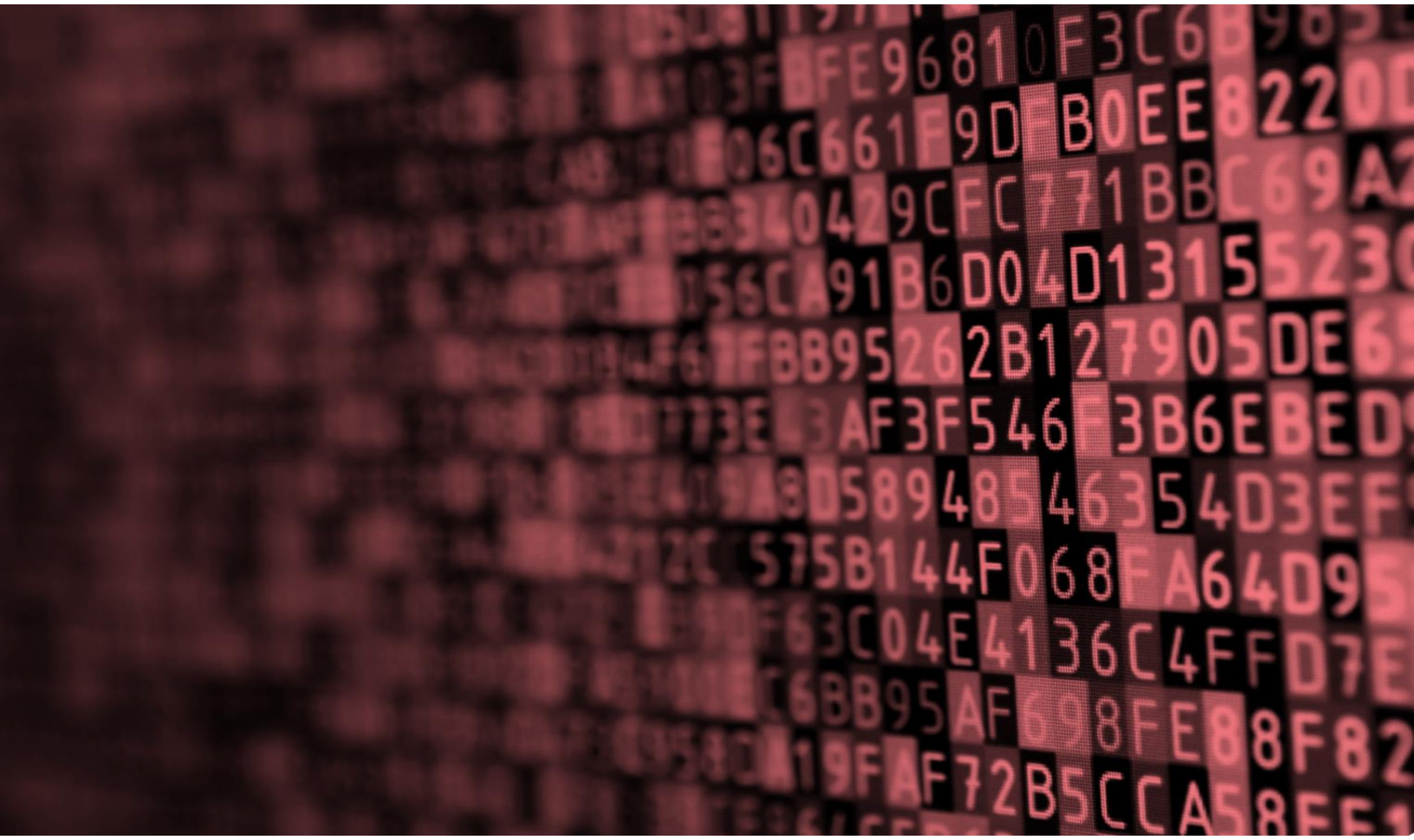

No Let-Up in PDPA Enforcement: PDPC Issues New Fines and Tightens Compliance Measures

Personal Data Protection Committee (PDPC) recently released a press statement addressing importance on laws concerning personal data protection, especially in cases where organizations collect, use or disclose a large amount of both sensitive personal data without implementing adequate security measures. They also issued administrative fines to private and public organizations for failing to implement adequate personal data security measures, notify the PDPC of personal data breaches and to appoint a Data Protection Officer as required under the Personal Data Protection Act (PDPA).

Following a previous case last year 2024 where a major e-commerce company was fined at 7 million Baht, the PDPC continued its enforcement in the year 2025, issuing penalties to both public and private entities that violated or failed to comply with the PDPA. This represents a significant milestone, emphasizing that data protection is more than just an internal management concern but a responsibility to safeguard citizens' fundamental rights.

The Expert Committee imposed administrative penalties for several cases. The summary of the cases are as follows:

1. Government Agency providing online public services via a web application: Failed to secure its web application, resulting in the leak of personal data of over 200,000 individuals to the dark web.

   Fine:
   - The government agency, as the Data Controller, was fined THB 153,120.
   - The system development company, as the Data Processor, was also fined THB 153,120.

2. A major private hospital: Patient medical records were repurposed as snack wrappers, leading to the leak of over 1,000 patient medical records.

   Fine:
   - The hospital, as the Data Controller, was fined THB 1,210,000.
   - The individual, as the Data Processor, was fined THB 16,940.

3. Three private e-commerce wholesale and retail Companies: Fined for failing to appoint a Data Protection Officer (DPO), notify the PDPC of personal data breaches, and implement adequate personal data security measures.

   Total Fines: In total of THB 13 million

In the next phase, the Ministry of Digital Economy and Society, in collaboration with the PDPC and its network partners, will undertake three main strategic focuses as follows:

1. Promoting the systematic appointment of Data Protection Officers (DPOs) across all organizations
2. Enhancing modern IT security infrastructure
3. Raising public awareness and understanding of their personal data rights.

These actions reflect the PDPC's ongoing and unwavering commitment to enforcing the Personal Data Protection Act. Organizations are urged to treat data protection not merely as a best practice, but as a legal and ethical obligation. Ensuring compliance must be a top priority, as failure to do so may result in significant legal and reputational consequences.

To navigate data protection risks and fortify your posture, implement these essential internal controls.

1. Robust Governance

Establish a clear framework of privacy policies for your organization and specific notices for data collection points. Appoint and empower a qualified Data Protection Officer (DPO) to lead compliance. Clearly define PDPA compliance roles and responsibilities across all departments.

2. Proactive Risk Management

Conduct a Data Inventory and Mapping (ROPA) to document all personal data. Perform Data Protection Impact Assessments (DPIAs) for new projects to assess privacy risks before they are implemented. Implement layered security measures—technical, organizational, and physical—to prevent data breaches.

3. Operational Controls

Establish streamlined consent management with a simple way for individuals to withdraw consent. Create clear procedures for handling data subject rights requests within legal timeframes. Mandate Data Processing Agreements (DPAs) with third-party vendors to define security and breach notification duties. Develop a data breach incident response plan for swift detection, containment, and notification.

4. Continuous Training

Implement mandatory and ongoing employee training tailored to each role. Foster a privacy-aware culture where data protection is a core organizational value, not just a compliance task.

5. Consistent Monitoring

Conduct regular internal audits to find and fix compliance gaps. Perform vulnerability assessments and penetration testing to proactively test security. Continuously review and update policies to stay aligned with evolving technologies and legal requirements.

By embedding these practical internal controls, organizations can significantly reduce their risk of PDPA non-compliance, protect data subjects' rights, and avoid the substantial financial and reputational costs seen in the recent enforcement actions.