

---

# Privacy Digest

---



AZURE DATA PROTECTION CONSULTANTS LLP

March 2025

Your Privacy Digest is filled with the latest developments in the field of privacy and data protection across the globe

# PRIVACY DIGEST



Welcome to this edition of our Privacy & AI Digest, where we bring you the latest developments in data privacy, AI regulations, and cybersecurity from around the world. In the U.S., Texas Attorney General Ken Paxton has launched an investigation into Chinese AI company DeepSeek over alleged ties to the Chinese Communist Party and potential violations of state privacy laws. Meanwhile, Canada's Privacy Commissioner has announced global privacy award winners, recognizing efforts in digital rights advocacy.

In Asia, Japan has introduced new AI regulations to balance innovation with misinformation control, and Malaysia has published its long-awaited data breach notification guidelines. The EU is grappling with uncertainties in trans-Atlantic data transfers following key dismissals in the U.S. Privacy and Civil Liberties Oversight Board. Stay informed as we dive deeper into these highlights and their impact on global privacy, security, and AI governance.



## **ASIA PRIVACY UPDATES**

### **Japan Issues AI Contract Checklist to Aid Businesses**

Japan's Ministry of Economy, Trade and Industry (METI) has released a Contract Checklist for the Use and Development of AI, aimed at helping businesses navigate legal and operational challenges in AI adoption. The checklist covers key issues such as AI usage scope, data security, liability, and service level agreements, ensuring fair risk allocation and responsible AI implementation. With AI adoption accelerating, METI seeks to provide businesses, especially those unfamiliar with AI legal frameworks, with practical guidance to mitigate risks and enhance compliance. The initiative is part of Japan's broader strategy to foster safe and competitive AI development in the global market.



### **Japan's Cabinet Approves AI Bill Promoting Research and Addressing Misinformation**



Japan's Cabinet has approved a new bill focused on promoting artificial intelligence (AI) research and development, recognizing its importance for national security. The legislation encourages the advancement of AI technologies while also emphasizing the need to address issues like misinformation. It includes provisions for investigating businesses that infringe on the public's rights, such as spreading false information, and recommending corrective actions. However, the bill does not impose legally binding sanctions, and the authority can only provide guidance or share information, with enforcement relying on existing regulations.

### **Vietnam Strengthens Data Protection with Stricter Regulations and Higher Penalties**

Vietnam has intensified its data protection measures with the issuance of Decree 24/2025/ND-CP on February 21, 2025, significantly increasing penalties for data privacy violations. Companies found mishandling consumer information, lacking user consent, or failing to address security breaches could face fines of up to VND 400,000,000. The decree also enforces stricter compliance requirements for digital platforms and B2C businesses, mandating robust data security, transparent policies, and prompt consumer complaint resolution. Organizations must take immediate action to ensure compliance through stronger security measures, regular audits, and clear data governance frameworks.



# PRIVACY DIGEST



## **EU PRIVACY UPDATES**

### **UK Unveils AI Playbook with 10 Principles for Public Sector AI Use**

The UK government has released an AI Playbook outlining ten principles to guide the responsible use of artificial intelligence in government and public sector organizations. The principles emphasize understanding AI's capabilities and limitations, ensuring lawful and ethical use, maintaining human oversight, managing AI securely, and selecting appropriate tools. Additionally, they stress collaboration, commercial engagement, skill development, and alignment with existing policies. The 118-page playbook serves as a comprehensive reference to help organizations navigate AI adoption while maintaining transparency, accountability, and security.



### **Uncertainty Over Trans-Atlantic Data Transfers Grows After PCLOB Dismissals**

The future of trans-Atlantic personal data transfers is under scrutiny following the recent dismissal of several members of the U.S. Privacy and Civil Liberties Oversight Board (PCLOB). The PCLOB is responsible for overseeing privacy-related activities of U.S. intelligence agencies and the functioning of the Data Protection Review Court, a key redress mechanism under the EU-U.S. Data Privacy Framework. The shake-up raises concerns about the framework's stability and its ability to meet EU privacy standards, potentially impacting data flows between the regions.



### **Ireland's DPC Investigates TikTok's EU-to-China Data Transfers**

Ireland's Data Protection Commission (DPC) has submitted a draft decision regarding its investigation into TikTok's transfer of EU users' personal data to China. The inquiry, launched in 2021, examines whether these transfers comply with the EU General Data Protection Regulation (GDPR). Other European data protection authorities now have a month to submit objections before a final ruling. The decision could set a significant precedent for data flows between the EU and China.





# PRIVACY DIGEST



## EU Unveils Cyber Blueprint for Large-Scale Cybersecurity Crisis Management

The European Commission has introduced a proposal for the Cyber Blueprint, a new EU framework aimed at strengthening cybersecurity crisis management. The nonbinding instrument seeks to enhance the EU's ability to respond to large-scale cyber incidents and follows the Commission's recent action plan to improve cybersecurity in hospitals and healthcare providers. The initiative highlights growing concerns over cyber threats and the need for a coordinated response across the EU.



## US PRIVACY UPDATES

### Texas Attorney General Launches Investigation Into DeepSeek Over Alleged CCP Ties

Texas Attorney General Ken Paxton has announced an investigation into DeepSeek, a Chinese AI company, over concerns about its alleged ties to the Chinese Communist Party (CCP) and potential violations of the Texas Data Privacy and Security Act. Paxton claims DeepSeek may be a "proxy for the CCP" aiming to undermine American AI leadership and compromise citizens' data. As part of the probe, he has issued Civil Investigative Demands (CIDs) to Google and Apple, seeking their analysis of the DeepSeek app. The Texas AG's Office has already banned DeepSeek's platform from its devices, citing security risks and censorship concerns. Paxton has shown strong inclination to take legal action against any CCP-linked company that threatens American technology and consumer privacy.



### Canada's OPC Launches Grants Program Focused on Smart Devices

The Office of the Privacy Commissioner of Canada (OPC) has opened its annual grants and contributions program, this year focusing on smart and connected devices. The initiative aims to fund research that explores privacy implications in emerging technology, with potential insights into improving digital assistants like Siri. Researchers and organizations are encouraged to apply, as findings could inform future privacy policies and technological advancements in consumer AI-driven devices.



# PRIVACY DIGEST



## Nova Scotia's Proposed Privacy Bill Draws Criticism Over Lack of Oversight

A proposed amendment to Nova Scotia's Freedom of Information and Protection of Privacy Act has sparked concerns over its lack of regulatory oversight. Critics argue that the draft bill fails to grant meaningful authority to the provincial Information and Privacy Commissioner, leaving key decisions such as whether a request is "vexatious" entirely up to the government. Privacy advocates warn that without independent oversight, the amendments may weaken transparency and accountability in the province's data protection framework.



## Canada's Privacy Commissioner Announces Global Privacy Award Winners

Canada's Privacy Commissioner Philippe Dufresne, in his role as Chair of the Global Privacy Assembly Working Group, has announced the winners of the first Global Privacy and Human Rights Award. The 5Rights Foundation and the Internet Freedom Foundation were recognized for their efforts in advocating digital privacy rights. 5Rights was honoured for its work on child privacy protections, while the Internet Freedom Foundation was acknowledged for promoting online privacy rights for workers and students. The awards highlight growing international efforts to strengthen privacy and digital freedoms.



## AI UPDATES

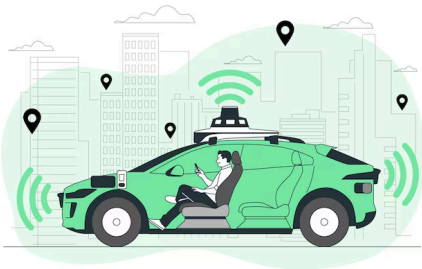
### **Australian Privacy Regulator Pushes Forward Amid Pre-Election Uncertainty**

Despite the usual slowdown in regulatory activity before a federal election, Australia's Office of the Australian Information Commissioner (OAIC) is forging ahead with key privacy initiatives. Information Commissioner Elizabeth Tydd announced preliminary inquiries into the privacy implications of connected vehicles and the development of a Children's Online Privacy Code. These efforts highlight the OAIC's commitment to addressing privacy concerns in evolving digital landscapes, including data collection by smart automobiles and safeguarding children's online interactions.



### **OAIC Investigates Privacy Risks of Connected Vehicles**

The OAIC has launched an inquiry into the privacy impacts of connected vehicles, which function as mobile data hubs. As modern cars collect and transmit vast amounts of user data, concerns are growing over data-sharing practices, consumer consent, and potential cross-border transfers of personal information. The investigation aims to establish clearer privacy expectations and align vehicle data policies with those applied to other connected devices, such as smartphones and smart TVs.



### **Australia Moves Forward With Children's Online Privacy Code**

In a significant step toward protecting minors in digital spaces, the OAIC is developing a Children's Online Privacy Code. The initiative aims to establish stricter guidelines for how online platforms collect, process, and use children's data. With parents balancing the need for digital literacy with concerns over online safety, the upcoming code will seek to provide a framework that enhances child privacy protections while fostering responsible internet use. The drafting process will be closely watched to see how regulators balance corporate responsibility with parental oversight.





## **FINES AND PENALTIES**

### **KakaoPay and Apple Pay Fined \$5.8M for Data Privacy Violations**

South Korea's Personal Information Protection Commission (PIPC) has fined KakaoPay and Apple Pay a combined \$5.8 million for violating the country's Personal Information Protection Act. The penalties stem from the unauthorized transfer of personal data from approximately 40 million users to Alipay between April and July 2018 without proper consent. The data, used to calculate NSF scores for payment evaluations, included phone numbers, email addresses, and account balances, even affecting users who had not registered Apple Pay. KakaoPay was fined \$4.14 million, while Apple Pay received a \$1.7 million penalty. Both companies must disclose the violations and implement compliance measures, while Alipay has been ordered to destroy its NSF score models based on the data. The ruling underscores the importance of transparency and regulatory compliance for global companies operating in South Korea.



### **Angel One Investigates Data Breach After Dark-Web Alert**

Angel One, a brokerage firm, reported unauthorized access to client data following alerts from its dark-web monitoring partner on February 27. Certain AWS cloud resources were compromised, prompting the company to immediately change credentials for its cloud and other applications. Angel One assured that client securities, funds, and credentials remain unaffected. The firm has engaged an external forensic partner to investigate the breach and conduct a thorough root cause analysis. Angel One emphasized its commitment to safeguarding clients' interests and continues to assess the potential impact while taking necessary security measures.



# PRIVACY DIGEST



## South Korea's PIPC Fines BusinessOn and NHN WIT for Major Data Breaches

South Korea's Personal Information Protection Commission (PIPC) has fined BusinessOn Communication and NHN WIT for data breaches affecting over 700,000 users. BusinessOn, operator of 'SmartBill,' suffered an SQL injection attack that exposed nearly 180,000 user records due to inadequate security measures, resulting in a penalty surcharge of 137 million won and fines of 2.7 million won. NHN WIT's fashion marketplace 'BagPop' was also hacked, leaking over 530,000 personal records, including resident registration numbers, due to insufficient security protocols and failure to destroy outdated databases, leading to a penalty surcharge of 61.1 million won and fines of 9.6 million won. Both companies have been ordered to strengthen security measures and publicly disclose the sanctions on their websites.





# Azure Data Protection Consultants LLP

Contact us for any queries:



<https://azuredpc.com/>



Azure Data Protection Consultants LLP



+91- 9599706305



[support@azuredpc.com](mailto:support@azuredpc.com)

## DISCLAIMER

This newsletter has been sent to you for informational purposes only and is intended merely to highlight issues. The information and/or observations contained in this newsletter do not constitute legal advice and should not be acted upon in any specific situation without appropriate legal advice. The views expressed in this newsletter do not necessarily constitute the final opinion of Azure Data Protection Consultants on the issues reported herein and should you have any queries in relation to any of the issues reported herein or on other areas of law, please feel free to contact us at [support@azuredpc.com](mailto:support@azuredpc.com).