Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

November 2024

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

PRIVACY DIGEST

India Cracks Down on Unauthorized PAN Data Use

In anticipation of the Digital Personal Data Protection Act coming into force, the government has intensified its scrutiny over the unauthorized use of Permanent Account Number (PAN) data by technology companies. This move is part of a broader effort to protect citizens' sensitive information as the new data protection law takes effect.

Recent directives have instructed financial and consumer technology firms to cease any unauthorized use of PAN data. Previously, some companies engaged in "PAN enrichment" practices—using citizens' PAN details to access additional personal data for customer profiling and targeted financial products. These practices often included accessing names, addresses, and contact details through backend systems, a practice now restricted under government oversight.

Approved services, such as those from the National Securities Depository, remain unaffected by this mandate. Authorized channels continue to provide limited verification services while ensuring compliance with regulatory standards. This crackdown highlights the government's commitment to secure data practices and limit access to citizens' personal information, allowing data to be processed only with explicit consent through sanctioned methods.

PRIVACY DIGEST

ASIA PRIVACY UPDATES

TRAI to Tighten Spam Call Regulations by January

TRAI plans to enforce stricter spam call and message regulations by January 2025. Recent actions include blacklisting 800 entities and disconnecting 1.8 million spam-linked numbers. New measures include higher tariffs for excessive calls/SMS, mandatory URL whitelisting in SMS for safety, and a Blockchain platform for tracking telemarketing calls. Full telemarketing transparency is required by December 1, with violations resulting in message rejections.

DSCI Highlights SaaS Benefits for Secure Access Management

The Data Security Council of India (DSCI) details the advantages of SaaS in its new paper, focusing on sectors like finance and healthcare. Key benefits include strengthened security, regulatory compliance, centralized identity management, continuous threat monitoring, and scalable cost efficiency. SaaS also supports multi-cloud strategies, manages privileged access, and uses AI for improved threat response.

Star Health Insurance Data Breach: Investigation Update

A data breach at Star Health Insurance exposed the personal information of approximately 31 million customers. Initial allegations implicated the Chief Information Security Officer (CISO) in selling data; however, the investigation found no evidence of involvement. Star Health is conducting a forensic investigation and secured a court order to remove leaked data from Telegram. The Insurance Regulatory and Development Authority of India (IRDAI) is monitoring the response and ensuring compliance with cybersecurity standards, highlighting vulnerabilities in data management within the insurance industry.

PRIVACY DIGEST

Hong Kong PCPD Issues Statement on Data Scraping Risks

On October 29, 2024, Hong Kong's Privacy Commissioner for Personal Data (PCPD), alongside international data protection authorities, issued a joint statement urging social media platforms and websites to protect publicly accessible personal data from unlawful data scraping. Highlighting risks like identity theft and cyberattacks, the statement stresses organizations' obligations to secure data and calls for transparency, consent, and responsible AI use in data handling practices.

CISA, FBI, and ACSC Issue New Guidelines for Secure Software Deployment

On October 25, 2024, CISA, the FBI, and Australia's ACSC issued guidance for secure software deployment across varied systems, including mobile devices, laptops, and cloud platforms. The guidance recommends a phased deployment process that prioritizes reliability, security, and minimal downtime, with steps covering risk assessment, rigorous testing, controlled rollouts, and ongoing post-deployment monitoring. It also includes protocols for continuous improvement, incident response, and encouraging users to adopt the latest software versions to maintain security.

New Zealand Privacy Commissioner Warns on Covert Filming Concerns

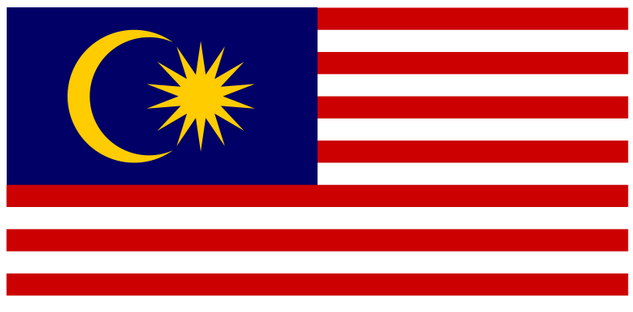
On October 22, 2024, New Zealand's Privacy Commissioner (OPC) raised concerns about increased camera use and covert filming. The OPC reported a surge in public queries about recording without consent, highlighting potential privacy violations and noting that covert filming may infringe on personal privacy rights. The OPC reminded the public of laws like the Harmful Digital Communications Act, which criminalizes sharing intimate recordings without consent, and advised on careful CCTV placement to avoid privacy issues.

PRIVACY DIGEST

OAIC Releases Privacy Guidance for Not-for-Profits

On October 22, 2024, Australia's OAIC published updated privacy guidance for not-for-profits, advising on secure data practices, retention and destruction obligations, and third-party management. Key points include collecting minimal data, secure storage, timely deletion, and thorough vendor oversight to ensure compliance.

Malaysia's Personal Data Protection (Amendment) Act 2024 Published



October 21, 2024, The Personal Data Protection (Amendment) Act 2024 was published in Malaysia, introducing mandatory data protection officers, compulsory data breach notifications, stricter penalties for non-compliance, and data portability rights. The Act enhances security requirements for data processors and will take effect on a date to be announced.

NCC Proposes Amendments for NGO Data Security Measures

October 4, 2024, The National Communications Commission (NCC) of Taiwan proposed amendments to enhance the security of personal data held by non-governmental organizations. Communication and broadcasting companies with annual revenues over NT $100 million or holding more than 100,000 pieces of personal data must disclose their anonymization techniques. They will also need to obtain verification for these techniques per the Personal Data Protection Act (PDPA) within one year of implementation.

Public Consultation on DPO Regulations in Sri Lanka

October 3, 2024, The Data Protection Authority of Sri Lanka has launched a public consultation on draft regulations for appointing a data protection officer (DPO) under the Personal Data Protection Act. A DPO is required for entities involved in regular monitoring or processing of sensitive personal data. Feedback on the draft is welcome until November 15, 2024.

PRIVACY DIGEST

개인정보보호위원회
Personal Information Protection Commission

PIPC Releases Guide on Personal Image Information

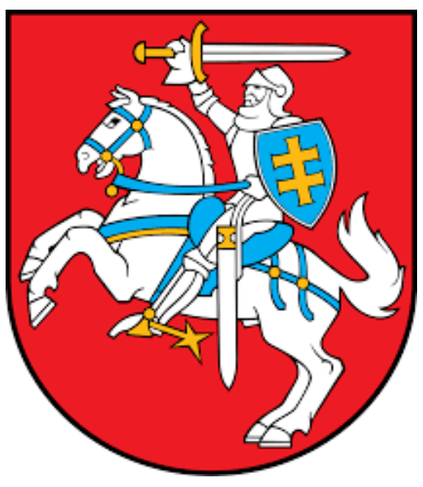
October 14, 2024, The Personal Information Protection Commission (PIPC) of South Korea has issued a guide on the protection and use of personal images captured by mobile devices in public areas. The guide establishes eight principles for processing personal data, focusing on compliance with the Personal Information Protection Act. It covers data collection, storage, and the rights of data subjects, while promoting pseudonymization in AI training, with certain research exceptions.

EU PRIVACY UPDATES

ICO Supports Data (Use and Access) Bill

October 31, 2024, The UK Information Commissioner's Office (ICO) has shown support for the Data (Use and Access) Bill, highlighting provisions related to smart data, cookie consent, international data transfers, and enhanced regulatory powers. The ICO calls for a 'Privacy-by-Design' approach and backs frameworks for digital verification and healthcare standards, while also endorsing clarified legitimate interests and safeguards for automated decision-making.

Information Commissioner's Office



VDAI Releases Training Materials for Data Protection Officers

On October 20, 2024, Lithuania's the State Data Protection Inspectorate (VDAI) published new training materials for data protection officers (DPOs). The materials cover legislative requirements for DPOs, video surveillance in public areas, implementing transparency principles, and guidelines for personal data security and risk assessment.

PRIVACY DIGEST

BSI Releases Guidance on Cyber Resilience Act

On October 21, 2024, the Federal Office for Information Security (BSI) published guidance on the Cyber Resilience Act (CRA). The guidance outlines that the CRA applies to digital products entering the EU market from late 2027, with exceptions for certain categories like medical devices. It details cybersecurity requirements, conformity declarations, and vulnerability disclosures, and also addresses implications for small and medium-sized enterprises (SMEs). A technical guideline for manufacturers will follow to clarify specific CRA requirements.

IMY Introduces New Regulations for Data Checks Against Sanctions Lists

On October 29, 2024, the Swedish Data Protection Authority (IMY) announced new regulations allowing certain companies to conduct personal data checks against sanctions lists without prior permission. This change benefits financial sector companies supervised by the Swedish Financial Supervisory Authority, as well as those in the security and defense sectors. The regulations take effect on November 1, 2024, and come with guidance from IMY for implementation.

France Introduces Senate Bill No. 33 for Cybersecurity Resilience

On October 15, 2024, the French Senate introduced Senate Bill No. 33 to transpose the NIS 2 Directive, the Critical Entities Resilience Directive (CER), and the Digital Operational Resilience Act (DORA) into national law. The bill expands the number of regulated entities from 600 to 15,000 and appoints the National Cybersecurity Agency for France (ANSSI) as the supervisory authority. It also mandates an online registration service for compliance. The Council of State confirmed the bill's alignment with the NIS 2 Directive on October 16, 2024.

PRIVACY DIGEST

Latvia's DVI Issues Guidance on Informing Data Subjects for GDPR Compliance

Data State Inspectorate Republic of Latvia

On October 1, 2024, the Data State Inspectorate (DVI) of Latvia released guidance for organizations on informing data subjects about data processing to ensure GDPR compliance. Organizations must provide transparent information on processing roles, purposes, and rights using various methods, including printed materials and visible notifications. While documentation of these efforts is necessary, obtaining acknowledgment from data subjects is not required.

SächsDSB Reports Data Protection Improvements Post-Audit

On October 27, 2024, the Saxon data protection authority (SächsDSB) revealed that after auditing 30,000 websites in May 2024, 1,500 operators enhanced their data protection measures. Notably, two-thirds ceased using Google Analytics without clear consent, and the number of cookies checked was halved. The SächsDSB warned that sanctions may follow for those still processing data illegally with Google Analytics and has provided support to 300 entities regarding compliance issues.

Norway Proposes Higher Consent Age for Social Media

On October 23, 2024, the Norwegian Government announced plans to raise the age limit for children's consent to social media data processing from 13 to 15 years. A consultation note will be released soon, stating that children under 15 should not use social media. The government is also considering legislation for a strict age limit, with the Norwegian Consumer Council supporting the initiative and advocating for thorough examination of the proposal and verification methods.

PRIVACY DIGEST

US PRIVACY UPDATES

DOJ Proposes Rule to Safeguard U.S. Sensitive Data

On October 21, 2024, the U.S. Department of Justice (DOJ) issued a Notice of Proposed Rulemaking (NPRM) to implement Executive Order 14117, which seeks to restrict access to sensitive U.S. personal and government data by certain countries, including China and Russia. The proposed rule defines prohibited transactions, establishes data sensitivity thresholds, and allows for specific exemptions. Public comments are welcome from October 29 to November 29, 2024.

FTC Introduces 'Click-to-Cancel' Rule for Easier Subscription Cancellations

On October 16, 2024, the FTC announced a new 'click-to-cancel' rule requiring sellers to make cancellation processes as simple as sign-ups. The rule, effective 180 days after publication, aims to prevent misleading marketing related to subscriptions and mandates clear disclosures and informed consent before billing.

EPIC Complains to FTC About OpenAI's Data Practices

On October 29, 2024, the Electronic Privacy Information Center (EPIC) filed a complaint with the FTC against OpenAI, alleging that the company used unauthorized web-scraping and stolen consumer data in the development of its AI products. EPIC claims these actions lead to significant privacy risks and biased outputs, violating the FTC Act. The complaint requests an investigation into OpenAI's practices and calls for compliance with established AI regulations.

PRIVACY DIGEST

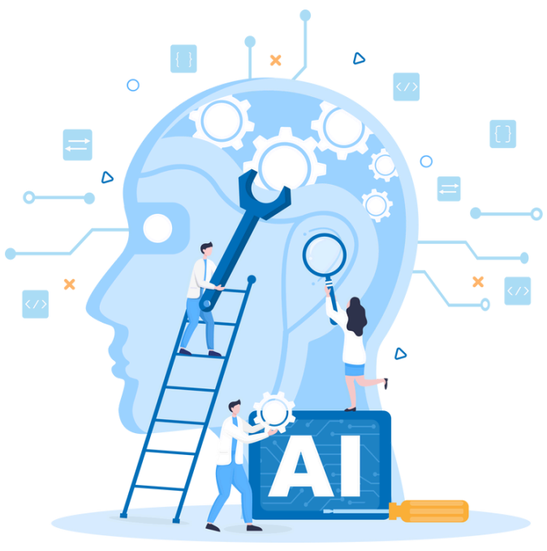
AI UPDATES

White House Launches AI Governance Framework for National Security

On October 24, 2024, the White House released a Framework for AI Governance and Risk Management in National Security. This initiative, part of Executive Order 14110, outlines guidelines for AI use in military operations, prohibiting discriminatory practices and constitutional rights violations. It mandates risk assessments, realistic testing, and operator training for high-impact AI applications, along with the establishment of an AI Governance Board and annual inventories of AI usage.

OAIC Issues AI Privacy Guidance for Developers

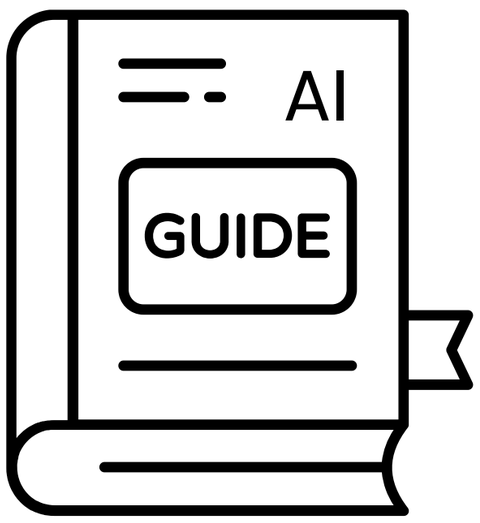
October 21, 2024, The OAIC released guidance for developers on privacy in generative AI development, highlighting that the Privacy Act 1988 applies to AI systems handling personal information. Key recommendations include ensuring data accuracy, assessing the legality of publicly available data, obtaining consent for sensitive data, and maintaining transparency with users. Checklists for privacy compliance throughout the development process are also provided.



OAIC Publishes Privacy Guidance for AI Developers

On October 21, 2024, the Office of the Australian Information Commissioner (OAIC) released guidance for developers on privacy considerations in generative AI. It clarifies that the Privacy Act 1988 applies to AI systems handling personal information. Developers are advised to ensure data accuracy, obtain explicit consent for sensitive data, and maintain user transparency. The guidance includes checklists for compliance, focusing on dataset selection and integrating privacy protections in the AI development process.

PRIVACY DIGEST



NAIC Publishes Guide on AI for ESG

Australia's National AI Centre (NAIC) released a guide on October 21, 2024, for ESG practitioners, highlighting AI's role in achieving sustainability goals like reducing deforestation and enhancing disaster response, while addressing risks like bias. The guide provides a framework for responsible AI use in ESG practices.

NYDFS Issues Guidance on AI Cybersecurity Risks

On October 16, 2024, the New York State Department of Financial Services (NYDFS) released guidance on managing cybersecurity risks related to artificial intelligence (AI). The guidance aims to assist entities in complying with existing Cybersecurity Regulations and outlines risks like AI-driven social engineering and heightened cyber threats. Recommendations include updating cybersecurity measures, conducting thorough due diligence on AI services, and improving threat detection and monitoring.

Harmonized Standards Set for EU Artificial Intelligence Act

On October 24, 2024, the European Commission's Joint Research Centre issued a policy brief on harmonized standards for the EU Artificial Intelligence Act. The brief emphasizes quality attributes such as risk prioritization, lifecycle coverage, and clarity. It outlines key deliverables related to risk management and human oversight, and identifies 37 standardization activities to ensure compliance with the AI Act by August 2026.

PRIVACY DIGEST

FINES AND PENALTIES

LinkedIn Fined €310 Million by Irish DPC for GDPR Violations

On October 24, 2024, the Irish Data Protection Commissioner (DPC) fined LinkedIn Ireland Unlimited Company €310 million for violating the GDPR. This action followed a complaint from La Quadrature Du Net to the French CNIL, leading to an inquiry that began in August 2018. The DPC found LinkedIn did not obtain valid consent for processing personal data for behavioral analysis and targeted advertising, which was deemed unlawful. The ruling also mandates LinkedIn to comply with GDPR requirements.

South Korea's PIPC Fines Neopharm for Data Breach and Privacy Violations

On October 24, 2024, South Korea's Personal Information Protection Commission (PIPC) fined Neopharm Co., Ltd KRW 105.17 million for violations of the Personal Information Protection Act (PIPA). Following a data breach in August 2023, where a hacker accessed Neopharm's systems 750 times and stole data of 293,723 individuals, the PIPC cited Neopharm's inadequate security practices and delayed user notification about the breach.

Vodafone Romania Fined for Email Data Breach

On October 28, 2024, the National Supervisory Authority for Personal Data Processing (ANSPDCP) imposed a fine of RON 24,870 (approx. $5,410) on Vodafone Romania S.A. for GDPR violations. The penalty followed a complaint about the unauthorized disclosure of personal email addresses during a change of account manager, attributed to the failure to use the Bcc option in emails. The ANSPDCP has mandated Vodafone to enhance its security measures and employee training to prevent future breaches.

PRIVACY DIGEST

ANSPDCP Fines UNTOLD SRL for GDPR Non-Compliance

On October 30, 2024, the ANSPDCP fined UNTOLD SRL RON 49,741 (about $10,860) for failing to address a data subject's access and deletion requests under the GDPR. The company did not respond to requests containing the individual's personal information, violating Articles 15 and 17(1). The authority also required UNTOLD to provide a written response to the data subject and implement GDPR compliance training for its staff.

Gums Dental Care Penalized $70,000 for HIPAA Noncompliance

On October 17, 2024, the U.S. Department of Health and Human Services (HHS) fined Gums Dental Care, LLC $70,000 for violating HIPAA Privacy Rules. The penalty arose after the dental practice failed to provide timely access to medical records despite multiple requests and reminders, not meeting the required 30-day response period.

Grue Municipality Fined for Data Breach

On October 29, 2024, Datatilsynet, Norway's data protection authority, fined Grue Municipality NOK 250,000 for a GDPR violation after sensitive pupil data was exposed in a public postal record. The breach included personal information such as names and social security numbers, with the municipality found lacking in required data processing protocols.

Ibercaja Banco Penalized for Unlawful Data Access Post-Contract

On October 22, 2024, Spain's data protection authority (AEPD) fined Ibercaja Banco €300,000, reduced to €180,000, for unlawfully accessing a customer’s file 47 times after their mortgage contract ended. The AEPD found this violated GDPR Article 6(1) due to the absence of a valid contractual relationship. The fine was lowered following Ibercaja's admission of liability and voluntary payment.

PRIVACY DIGEST

DATA BREACH

Cisco Confirms Data Theft from DevHub Environment

On October 21, 2024, Cisco confirmed a data theft incident after a hacker, IntelBroker, claimed to have stolen files from its public DevHub environment. The hacker alleged access to source code and internal documents related to major companies, but Cisco stated that its main systems remain secure and no sensitive personal or financial information has been compromised. The investigation is ongoing, and public access to the affected site has been disabled.

Interbank Data Breach Exposed Sensitive Customer Data

On October 30, 2024, Interbank confirmed a data breach involving the exposure of sensitive information from over 3 million customers, including names, account details, and credit card information. The breach was linked to a hacker who leaked the data online after failed extortion attempts. Despite some service outages, Interbank assures clients that their deposits remain secure and is enhancing security measures to protect customer information.

Landmark Admin Data Breach Affects 800,000 U.S. Customers

Landmark Admin has confirmed a data breach affecting over 800,000 customers in the United States, exposing sensitive information such as Social Security numbers and driver's license details. The breach, initially detected on May 13, 2024, involved unauthorized access and data theft. In response, Landmark is providing free identity theft protection services and notifying affected individuals by mail, starting October 23, 2024.

PRIVACY DIGEST

Saint Xavier University Reports Data Breach Affecting Over 200,000 Individuals

On October 30, 2024, Saint Xavier University (SXU) reported a data breach affecting 212,267 individuals, compromising sensitive information including names, Social Security numbers, and financial account details. The breach was detected on July 21, 2023, after unauthorized access to the university's network occurred between June 29 and July 18, 2023. Following an investigation, SXU began notifying affected individuals about the compromised information on October 30, 2024.

Free ISP Data Breach Exposes Millions of Customers

On October 28, 2024, Free, France's second-largest internet service provider, confirmed a data breach impacting approximately 19.2 million customers. The compromised data includes over 5.11 million IBAN numbers, but no passwords or financial details were leaked. The company has notified authorities and is enhancing security measures. Customers are advised to monitor their accounts for unusual transactions and remain vigilant against phishing scams.

Henry Schein Data Breach Impacts 166,432 Customers

On October 24, 2024, Henry Schein revealed that a data breach linked to cyberattacks by the BlackCat Ransomware gang in 2023 affected the personal information of 166,432 individuals. The company, a healthcare solutions provider, had to take systems offline to address the breaches. Details on the specific data stolen are not fully disclosed, but impacted individuals are being offered a free 24-month subscription to Experian's IdentityWorks for credit monitoring and fraud detection.

Azure Data Protection Consultants LLP

Contact us for any queries:

https://azuredpc.com/

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com

DISCLAIMER