Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

August 2024

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

AUGUST 2024 — AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

Welcome to Our Latest Newsletter

As data collection and sharing become more prevalent, integrating privacy into every aspect of technology is increasingly important. Privacy by Design embeds privacy from the start, making it a core part of system and technology development.

In this issue, we cover an important update: the rules for the Digital Personal Data Protection (DPDP) Act are expected to be released by the end of the current Parliament session. These rules might introduce exemptions for certain institutions, require immediate notification of data breaches to the Data Protection Board, and place the responsibility on platforms to verify consent for processing children's data.

We'll keep you informed about these changes and offer insights on incorporating Privacy by Design principles into your work. Whether you're involved in technology, data management, or simply value your personal privacy, we're here to support you in making privacy a key focus in all your projects.

Thank you for joining us as we explore how to make privacy an essential part of innovation and design.

PRIVACY DIGEST

ASIA PRIVACY UPDATES

Social Media Giants Concerned Over India's Data Law

Tech giants like Google, Meta, YouTube, and Snap are worried that India's new Digital Personal Data Protection (DPDP) Act could harm child safety online. The Act's restrictions on behavioral tracking and its requirement for verifiable parental consent may affect their ability to protect young users. Companies are calling for exemptions and clearer guidelines to ensure both privacy and effective safety measures.

DPDP Rules Expected by End of Parliament Session for Public Consultation

The rules for India's Digital Personal Data Protection (DPDP) Act, passed in August 2023, are anticipated to be released by the end of the current Parliament session, potentially by August 12, 2024. The draft rules will address exemptions for certain institutions, mandate that data fiduciaries promptly notify the Data Protection Board of breaches, and clarify provisions related to children's data, including age verification and parental consent. The rules will undergo a month-long public consultation before finalization.

India's Supreme Court Rules Google Pin Sharing as Bail Condition Violates Privacy

On July 8, 2024, India's Supreme Court determined that a bail condition requiring the accused to share their location via Google Maps violates their right to privacy under Article 21 of the Constitution. The Court found this condition to be an unnecessary form of surveillance, noting that Google's pin-sharing feature only marks a static location and does not allow real-time tracking. The ruling emphasizes that bail conditions must respect privacy rights and be relevant to the trial process.

PRIVACY DIGEST

Japan's PPC Announces Interim Summary on APPI Amendments

Japan's Personal Information Protection Commission (PPC) released an "Interim Summary" on June 27, outlining proposed changes to the Act on the Protection of Personal Information (APPI). Key updates include new rules for biometric data, stricter unauthorized data use regulations, enhanced opt-out requirements for third-party data, and specific regulations for children's data. The draft law will be available in 2025 with implementation in 2027. Public comments are open until July 29.

China's New Data Export Rules

China's updated data export regulations require foreign companies to proactively identify and declare important data. Instead of waiting for notifications, firms must work with regulators to confirm data and file a cross-border data transfer (CBDT) application with the CAC for export. Compliance with these new rules is essential to avoid penalties.

Singapore's PDPC Issues Guide on Synthetic Data Generation

On 15 JULY, 2024 Singapore's Personal Data Protection Commission (PDPC) released a guide on synthetic data generation, titled "Privacy Enhancing Technology (PET): Proposed Guide on Synthetic Data Generation." The guide offers recommendations for creating and using synthetic data—data generated through algorithms that mimic real data without revealing personal information. It highlights the benefits of synthetic data for AI model training, data sharing, and software testing while addressing risks like re-identification.

PRIVACY DIGEST

AMERICA PRIVACY UPDATES

US Sues TikTok Over Privacy Violations of Children Under 13

On August 2, the U.S. Justice Department sued TikTok and its parent company ByteDance for allegedly violating the Children's Online Privacy Protection Act by improperly collecting data from users under 13 without parental consent. The lawsuit, supported by the FTC, seeks substantial penalties and reflects broader concerns about TikTok's data practices and its potential connections to the Chinese government. TikTok disputes the claims, stating they are based on outdated or incorrect information.

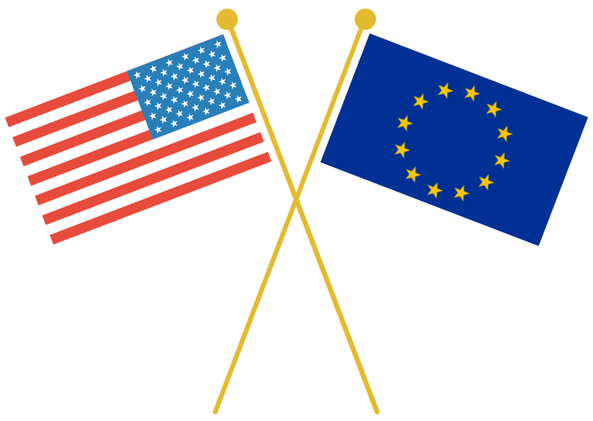
New York's Newly Passed Child Data Protection Act

New York's newly passed Child Data Protection Act regulates the collection and processing of data from users under 18. Effective in one year, it requires explicit consent for data processing and affects third-party cookies and data sales. The law mandates updates to privacy practices and will be enforced by the New York Attorney General.

CrowdStrike Update Causes Global Outage

On July 19, 2024, CrowdStrike's software update led to a widespread outage affecting global banks, airlines, and government offices. The update, which aimed to enhance security, contained faulty code, resulting in system crashes. Security experts suggest the code may not have been properly vetted. In a related development, Alphabet's CapitalG had already reduced its stake in CrowdStrike before the outage, a move that has gained attention following the incident. CrowdStrike shares have dropped nearly 35% since the outage, and Delta Air Lines, one of the affected companies, is pursuing legal action against CrowdStrike and Microsoft for the disruptions.

PRIVACY DIGEST



US and European Regulators Sign Joint AI Competition Statement

Regulators from the US, European Union, and UK have signed a joint statement to promote fair competition in the rapidly evolving artificial intelligence (AI) sector. The agreement outlines principles to protect consumers and ensure a level playing field as AI technology advances. Key agencies, including the European Commission and the US Federal Trade Commission, emphasized their commitment to preventing anti-competitive practices in the AI industry.

Brazil Bans Meta from Using Local Data to Train AI Models

On July 2, 2024, Brazil's national data protection authority prohibited Meta from using data from Brazilian users to train its AI systems. The ban affects Meta's plans to utilize public posts from Facebook and Instagram for AI development. This decision is based on concerns over potential harm to users' rights and privacy. Despite Meta's statement that their practices comply with local regulations, the ban aims to safeguard user data from being exploited for AI without proper consent. Meta must comply within five days or face a daily fine of 50,000 reais ($8,820).

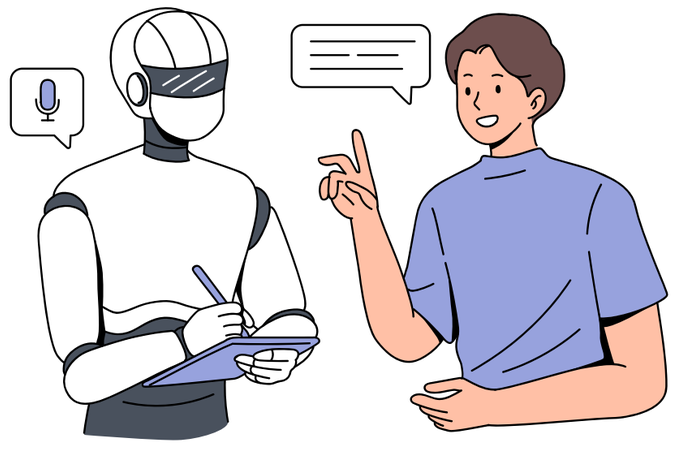
ANPD Releases New Regulation on the Role of Data Protection Officer

Brazil’s ANPD has released new rules for Data Protection Officers (DPOs) under the LGPD. DPOs can now be individuals or entities, must communicate in Portuguese, and all data controllers are required to appoint one. The regulation highlights DPO autonomy, conflict-free roles, and public contact details. Small controllers and processors are exempt but encouraged to appoint a DPO. The ANPD will offer further guidance, with a meeting on August 1 to address additional issues.

PRIVACY DIGEST

AI UPDATES

Bollywood Singer Arijit Singh Wins Legal Battle Against AI Voice Mimicking

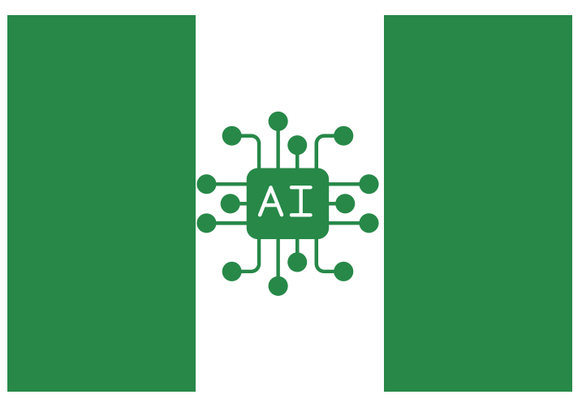


The Bombay High Court has ruled in favor of Bollywood singer Arijit Singh, granting him interim relief in his lawsuit against AI platforms that used his voice without permission. The court recognized Singh's personality rights, including his voice, likeness, and image, as protectable under copyright law. This ruling highlight the misuse of AI to exploit personal identity for commercial purposes without consent, potentially harming Singh's career and reputation. The case underscores the need for legal protections against unauthorized use of celebrity identities in the digital age.

AI Act Now in Effect

As of August 1, 2024, the European Artificial Intelligence Act (AI Act) is officially in force. This landmark regulation introduces a risk-based framework for AI in the EU, classifying AI systems into categories ranging from minimal to unacceptable risk. It mandates strict requirements for high-risk applications while banning certain uses that threaten fundamental rights. Additionally, the EU has launched consultations on a forthcoming Code of Practice for general-purpose AI models, with a final version expected by April 2025.

Nigeria Launches National AI Strategy to Drive Local Innovation



Nigeria's "National AI Strategy" outlines a vision for leveraging AI to tackle local challenges and spur innovation. The strategy advocates for homegrown AI solutions tailored to Nigeria's needs, highlighting opportunities in agriculture and public health. It acknowledges the importance of addressing data collection and quality issues to develop effective AI systems, aiming to position Nigeria as a leader in AI across Africa.

PRIVACY DIGEST

CNIL's New Guidelines for Generative AI Deployment

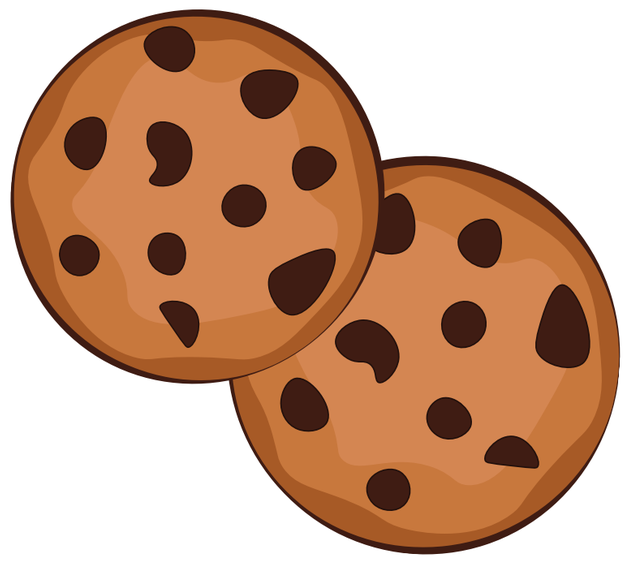
On July 18, 2024, CNIL released new guidelines for deploying generative AI systems with a focus on data protection. Key recommendations include using AI for specific purposes only, avoiding personal data input, acknowledging AI's limitations, and ensuring secure deployments. Organizations are advised to educate users, ensure GDPR compliance, and consider secure, on-premise solutions for sensitive data. Continuous monitoring and involving data protection officers are also emphasized to address emerging risks and maintain transparency.

NIST Issues New Guidance on Generative AI Risks

NIST has released the AI RMF Generative AI Profile (NIST AI 600-1), which outlines over 200 risk management actions for generative AI. The guidance addresses key issues such as cybersecurity threats, content inaccuracies, and privacy concerns, emphasizing the need for strong governance, risk assessment, and continuous monitoring. This profile enhances the existing AI Risk Management Framework by providing specific strategies for managing the unique challenges of generative AI.

Google Halts Plan to Remove Cookies from Chrome

Google has reversed its decision to phase out third-party cookies from its Chrome browser, despite years of pledging to do so. The move comes after concerns from advertisers, who rely on cookies for personalized ads, and scrutiny from regulators like the UK's Competition and Markets Authority. Instead of removing cookies, Google will introduce new privacy controls in Chrome, allowing users to manage their preferences. The decision has sparked mixed reactions, with some praising the relief for advertisers and others criticizing the potential privacy risks.



PRIVACY DIGEST

FINES AND PENALTIES

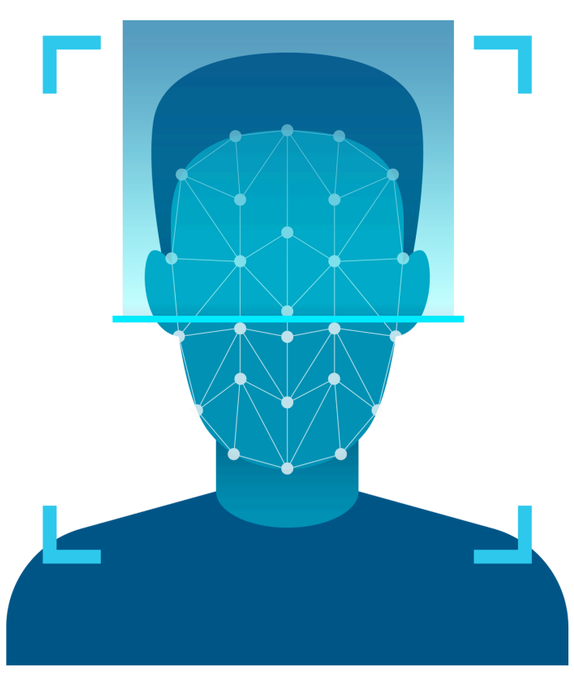
PIPC Fines AliExpress $1.43 Million for PIPA Violations

South Korea's Personal Information Protection Commission (PIPC) has fined AliExpress 1.978 billion KRW (USD 1.43 million) for violating the Personal Information Protection Act (PIPA). The e-commerce giant failed to provide adequate data protection and transparency for cross-border transfers involving over 180,000 Korean users. The PIPC's ruling includes a financial penalty and corrective orders to enhance data privacy measures.

Nigeria Fines Meta $220 Million for Data Law Violations

Nigeria has fined Meta $220 million for violating consumer and data protection laws. The Federal Competition and Consumer Protection Commission (FCCPC) found that Meta improperly used Nigerian users' data without consent and imposed exploitative privacy policies. The investigation, conducted with Nigeria's Data Protection Commission, concluded that Meta's practices were abusive and invasive. Meta has yet to comment but has engaged with the FCCPC during the process. The fine also includes steps Meta must take to comply with local laws moving forward.

Meta to Pay $1.4 Billion Over Facial Recognition Privacy Violations



Meta, the parent company of Facebook and Instagram, has agreed to pay $1.4 billion to Texas to settle a lawsuit over the illegal collection of facial recognition data. Texas Attorney General Ken Paxton announced the settlement, the largest privacy settlement by a U.S. state, following allegations that Meta violated state privacy laws by automatically tagging users' faces. This settlement highlights growing state-level enforcement of privacy laws, especially as federal privacy regulations remain absent. Texas' biometric privacy law mandates that companies obtain permission before using facial or voice recognition technologies.

PRIVACY DIGEST

RANSOMWARE/DATA BREACH

Ransomware Attack Shuts Down Hundreds of Small Indian Banks

A ransomware attack on C-Edge Technologies, a banking technology provider, has forced nearly 300 small Indian banks offline, disrupting their payment systems. The National Payment Corporation of India (NPCI) has temporarily isolated C-Edge from the broader payment network to prevent further spread. Affected banks, mostly cooperative and regional institutions, account for about 0.5% of the country's payment volume. The Reserve Bank of India and NPCI are auditing the situation to contain the impact, while C-Edge has not yet commented on the incident.

WazirX Hacked; $230 Million Stolen in Major Security Breach

On July 18, India’s largest cryptocurrency exchange, WazirX, suffered a major security breach, resulting in the theft of $230 million in digital assets. The attack, suspected to involve North Korea, compromised a multisig wallet, leading WazirX to pause withdrawals and trading. The exchange filed a police complaint the next day, and an FIR was registered on August 5 in New Delhi. WazirX is working with authorities to recover the stolen funds and improve user security.

Ransomware Attack Disrupts OneBlood; Operations Fully Restored

Following a ransomware attack on July 29, OneBlood's operations were initially hampered, leading to a switch to manual processes. The organization has now restored normal operations, and blood distribution is back to its regular schedule. OneBlood urges donors to schedule appointments to maintain adequate blood supplies.

PRIVACY DIGEST

Los Angeles County Superior Court Resumes Operations After Ransomware Attack

The Los Angeles County Superior Court has reopened as of July 23 following a ransomware attack that closed all 36 courthouses on July 19. Although systems are back online, users may experience delays and disruptions as the court continues to restore full functionality.

Hackney Council Reprimanded for Ransomware Failures

On 17 July, 2024, the ICO reprimanded Hackney Council for its mishandling of a ransomware attack in October 2020. Security failures, including unpatched systems and weak passwords, resulted in over 400,000 files being encrypted and services disrupted for almost two years. The ICO opted for a reprimand instead of a fine due to the council's mitigation efforts. Hackney Council disputes the findings, asserting that they did not breach security obligations.

4.3 Million Affected in HealthEquity Data Breach

On August 1, 2024, HealthEquity disclosed a March 9 breach that impacted 4.3 million individuals. Unauthorized access to a partner's account led to the compromise of personal data including names, addresses, and Social Security numbers. Discovered on June 26, HealthEquity is offering identity theft protection and has enhanced its security.

PRIVACY DIGEST

Singapore Ministry of Law Confirms Data Breach Affecting 128,000 Borrowers

On July 25, 2024, Singapore's Ministry of Law confirmed a data breach affecting 12 licensed moneylenders and 128,000 clients. Hackers, identified as GhostR, accessed personal and financial data via a third-party IT vendor, Ezynetic Pte Ltd. The data, including loan details and borrower histories, was leaked on a hacking forum after GhostR's demands were not met. The Moneylenders Credit Bureau and Credit Bureau (Singapore) have restricted access to mitigate further risk, and investigations are underway.

Australia: Children's Personal Photos Misused to Power AI Tools

Human Rights Watch found that photos of Australian children are being used without consent to train AI tools, leading to risks like deepfakes and privacy breaches. The LAION-5B dataset, which includes identifiable images of children, contributes to these issues. Human Rights Watch calls for stronger legal protections, including Australia's proposed Children's Online Privacy Code, to safeguard children's data from misuse.

Azure Data Protection Consultants LLP

Contact us for any queries:

https://azuredpc.com/

Azure Data Protection Consultants LLP

+91- 9599706305

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.