Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

July 2024

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

JULY 2024

AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

LATEST TRENDS

Welcome to our July Newsletter, your go-to source for the latest developments in data privacy, security, and technology regulation. In this edition, we bring you a comprehensive overview of the most recent reports, legislative changes, and technological advancements impacting privacy across India and the globe.

Stay informed about key updates, including India's progress in Privacy-Enhancing Technologies. This issue also delves into the rapidly evolving landscape of AI governance, offering insights into the latest regulatory frameworks, compliance guidelines, and high-profile legal battles in the AI domain.

Whether you're a privacy professional, technology enthusiast, or concerned citizen, our newsletter provides essential information to help you navigate the complexities of data privacy in today's digital world. Dive in to explore how global privacy practices are shaping the future of technology and regulation.

Enjoy reading, and stay updated with the latest privacy news from around the world.

PRIVACY DIGEST

INDIA PRIVACY UPDATES

DSCI Releases Report on PETs

The Data Security Council of India (DSCI) recently published a report on Privacy-Enhancing Technologies (PETs), examining their regulatory status in India and ten other jurisdictions worldwide. The report categorizes PETs into five types and underscores their role in building consumer trust and ensuring compliance with laws such as the Digital Personal Data Protection Act, 2023. It proposes integrating PETs into robust data governance platforms for effective regulatory compliance.

DSCI publishes paper on curbing scams in UPI

Released on June 4, 2024, a comprehensive white paper addresses the escalating issue of scams within India's Unified Payments Interface (UPI). It outlines strategies to tackle unauthorized transactions (AbU) and other fraudulent activities, emphasizing the need for a Comprehensive Fraud Reporting and Management System (CFRMS). The CFRMS aims to streamline scam reporting channels, standardize data collection, and enhance intelligence for effective enforcement actions. By fostering dialogue among policymakers, industry stakeholders, and the public, the white paper aims to bolster UPI's security framework and potentially influence global standards for secure digital payments.

PRIVACY DIGEST

UK PRIVACY UPDATES

ICO and OPC Launch Joint Investigation into 23andMe Data Breach

The UK Information Commissioner's Office (ICO) and the Office of the Privacy Commissioner of Canada (OPC) have jointly launched an investigation into a data breach at 23andMe, occurring in October 2023. This breach involved sensitive genetic information, prompting concerns about potential harms and the adequacy of 23andMe's security measures. Both offices will assess the scope of the breach, compliance with data protection laws regarding notification, and the safeguarding of personal information. The investigation underscores their commitment to protecting privacy rights globally, with updates to follow upon its conclusion.

UK Train Stations Trial Amazon Emotion Detection

Eight UK train stations, including major hubs like London's Euston and Waterloo, used Amazon's AI surveillance to analyze passengers' age, gender, and emotions via CCTV cameras. Big Brother Watch raised concerns over privacy and transparency, criticizing Network Rail for deploying the technology without public awareness. The initiative aimed to enhance safety but sparked debates over the ethical use of AI in public spaces.

PRIVACY DIGEST

EU PRIVACY UPDATES

Balancing Security and Privacy: New EU Encryption Report

The EU Innovation Hub for Internal Security has published a report on encryption, emphasizing the balance between privacy and criminal investigation needs. With contributions from Europol, Eurojust, and other EU bodies, the report highlights encryption's role in both protecting communications and enabling crime. Key points include the need for legal frameworks for data access, collaboration with academia and industry, and addressing advanced technologies like quantum computing and AI. This initiative aims to ensure security while safeguarding rights.

LinkedIn Ceases Targeted Ads Using Special Category Data

As of June 7, 2024, LinkedIn has halted a targeted advertising feature following an inquiry from the European Commission under the Digital Services Act (DSA). The inquiry raised concerns about LinkedIn potentially allowing advertisers to target users based on sensitive special category data, such as race or health information, which is protected under GDPR. LinkedIn's decision aligns with the DSA's prohibition on such practices, emphasizing the importance of respecting user privacy and complying with stringent data protection regulations. Stay updated for further developments on LinkedIn's compliance efforts and regulatory responses.

PRIVACY DIGEST

EU and Australia Boost Digital Cooperation

The European Union and Australia held their second Digital Dialogue, focusing on enhancing digital cooperation and innovation. They agreed to increase collaboration on platform regulation and signed an Administrative Agreement to enforce social media rules. Discussions included sharing AI governance experiences and promoting a secure, human-centric data economy. Cybersecurity cooperation, including protection of critical infrastructure and addressing ransomware, was also a priority. Led by senior officials like Roberto Viola from the European Commission, the dialogue highlighted commitments to a resilient global digital environment.

CANADA PRIVACY UPDATES

EU Renews Canada's Data Adequacy: The Path Forward for Bill C-27

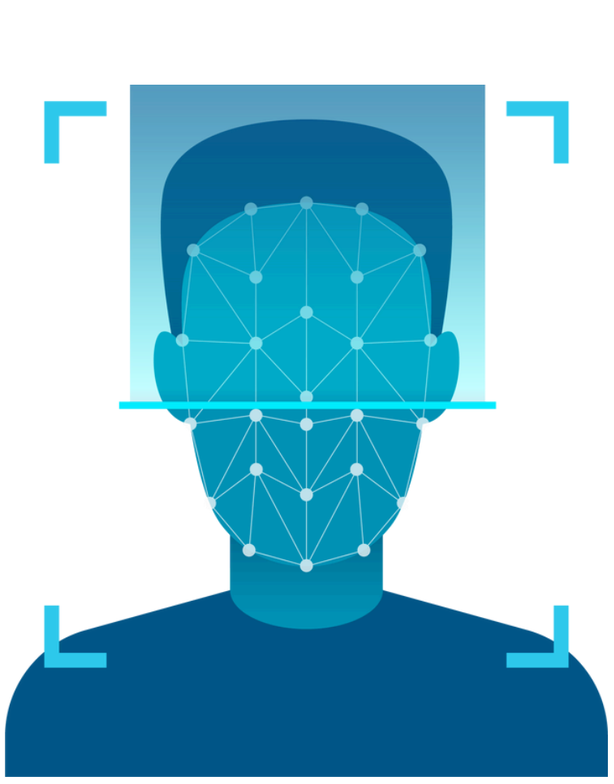
On January 15, the European Commission renewed data adequacy for 11 nations, including Canada, which is updating its privacy laws with Bill C-27. With elections looming in October 2025, stakeholders doubt C-27 will pass in time. The Commission recommended embedding certain protections into federal law, highlighting Canada's efforts to modernize PIPEDA. Privacy Commissioner Philippe Dufresne praised the renewal, while nNovation Counsel Constantine Karbaliotis criticized it for reducing legislative urgency. Bill C-27, including the Consumer Privacy Protection Act, the Tribunal Act, and the AI Data Act, is under review. If passed, it will take effect in 18-24 months. Minister François-Philippe Champagne emphasized the importance of updated privacy laws and AI regulation. Some suggest separating the AI Data Act for faster passage. Companies are adapting to Quebec's Law 25, indicating a shift in privacy compliance. The future of C-27 remains uncertain, but modernization efforts continue.

PRIVACY DIGEST

US PRIVACY UPDATES

US Bans Kaspersky Antivirus

The Biden administration has announced a ban on Kaspersky Lab antivirus software in the US, citing security risks due to the company's ties to Russia. Commerce Secretary Gina Raimondo highlighted that Kaspersky's software could be exploited to steal information or install malware, threatening critical infrastructure and government entities. Effective September 29, the ban will halt sales, updates, resales, and licensing of Kaspersky products. This move is part of broader efforts to counter Russian cyber threats and pressure Moscow amidst the Ukraine conflict. Kaspersky denies the claims and plans to pursue legal action. Businesses have 100 days to find alternatives, and violators could face fines or criminal charges.



FTC Cracks Down on AI: Essential Compliance Insights

Recently, the U.S. Federal Trade Commission (FTC) banned Rite Aid from using facial-recognition technology for five years due to biases that unfairly targeted women and people of colour. This highlights the need for companies to implement responsible AI governance and ethical practices. The FTC is actively addressing market issues, deceptive practices, and invasiveness in AI tools, emphasizing data security and transparent development. To navigate this landscape, companies should align AI policies with practical implementation, ensure honest claims about AI capabilities, and integrate privacy, security, and ethics into every stage of AI development to build trust and mitigate risks.

PRIVACY DIGEST

US lawsuit against TikTok to focus on children's privacy

June 21 - The U.S. Department of Justice plans to sue TikTok for allegedly violating children's privacy rights, focusing on claims that the platform mishandled young users' data. This lawsuit, recommended by the U.S. Federal Trade Commission after its investigation, moves forward despite TikTok's disagreement with the allegations. This case is distinct from ongoing congressional concerns about potential Chinese government access to data from TikTok's 170 million U.S. users. Additionally, TikTok is challenging a law requiring its parent company ByteDance to divest its U.S. assets by January 19 or face a ban.

Colorado Passes Landmark Mind Privacy Law

Colorado has enacted a pioneering law to protect against the privacy risks posed by advancing mind-reading technology. Dr. Sean Pauzauskie of UCHealth led the initiative, highlighting the benefits and risks of neurotechnology devices. The law, effective August 8, adds brain data to Colorado's State Privacy Act, aiming to safeguard sensitive information from potential misuse by insurers, law enforcement, and other entities. Pauzauskie calls for broader federal and global regulations to ensure the protection of thoughts, emotions, and memories in an increasingly interconnected world.

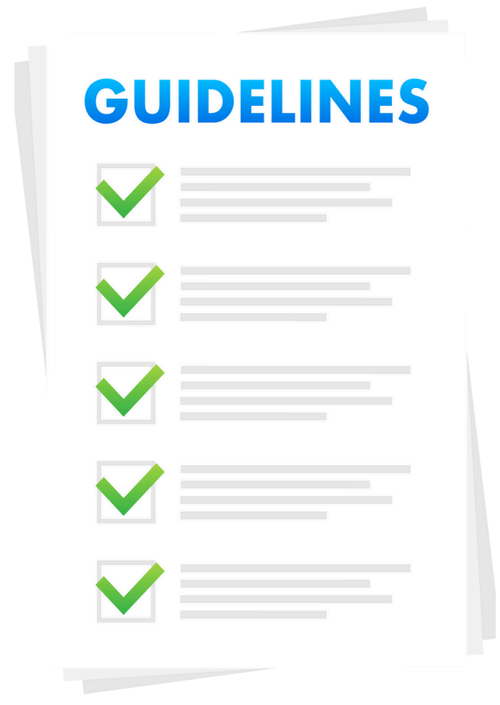
New York Senate Advances Bill Creating Chief AI Officer

The New York State Senate recently passed Senate Bill No. 9104, marking a significant step towards establishing a chief artificial intelligence (AI) officer under the state technology law. This officer will lead the Office of AI, tasked with developing statewide AI policies, coordinating AI activities across governmental bodies, and ensuring compliance and oversight of AI tools and automated decision-making systems. The bill underscores New York's commitment to proactive regulation and governance of AI technologies, aiming to enhance transparency and accountability in their implementation across public sectors.

PRIVACY DIGEST

CHINA PRIVACY UPDATE

China's Updated Data Guidelines



China has recently released revised guidelines to streamline the handling of sensitive personal information. These guidelines aim to strike a balance between protecting privacy and supporting economic goals. They provide clearer rules on data processing and cross-border transfers. However, they do not address concerns regarding government access to personal data, which remains a focal point for critics and analysts.

ETHIOPIA PRIVACY UPDATE

Ethiopia’s Commercial Bank Under Fire for Data Privacy Violations

The Commercial Bank of Ethiopia faces backlash for publishing customers' names and photos to recover $14 million lost in an ATM glitch. Critics, including Access Now and Ethiopia’s Centre for Advancement of Rights and Democracy, argue this violated privacy rights. Following criticism, the bank removed the information after recovering 99% of the funds. The incident has intensified calls for stronger data protection laws in Ethiopia, highlighting ongoing concerns about privacy practices in state-owned entities.

PRIVACY DIGEST

AI UPDATES

New OECD Report on AI, Data Governance & Privacy

The OECD's new report, "AI, Data Governance and Privacy - Synergies and Areas of International Cooperation," is essential reading for privacy and AI enthusiasts. It covers the intersection of Privacy Enhancing Technologies (PETs) and AI, including a section on generative AI and machine unlearning, Machine unlearning is another emergent subfield of machine learning that would grant individuals control over their personal data, even after it has been shared. The report also examines OECD principles on privacy and AI, national and regional developments, and the legal challenges of interpreting legitimate interest requirements in AI. It highlights the need for more cooperation between AI and privacy communities.

Governing with AI: OECD Report Explores Policy Challenges and Opportunities

The OECD has released a new report titled "Governing with Artificial Intelligence - Are governments ready?" which examines key trends and policy challenges surrounding AI adoption in the public sector. The report underscores AI's potential benefits for enhancing government productivity, responsiveness, and accountability. It highlights examples of AI applications across OECD countries aimed at improving internal operations and public service delivery. However, it also emphasizes the need for responsible AI deployment to mitigate risks such as bias amplification, transparency concerns, and data privacy breaches. The report calls for more evidence-based insights to guide successful AI initiatives, stressing the importance of ethical considerations in sensitive policy domains like law enforcement and welfare benefits.

PRIVACY DIGEST

Australia's New AI Governance Framework: Guiding Principles for Public Sector Innovation

Australia has introduced its "National framework for the assurance of AI in government," a pivotal document for AI professionals, public administrators, and policymakers. Emphasizing adaptive governance structures and accountability frameworks, the framework guides decision-making around AI deployment in government functions. It advocates for discretion in system development, prioritizing traceability and establishing feedback mechanisms to mitigate risks. The framework also integrates Australia's AI Ethics Principles, focusing on fairness, transparency, and accountability.

Record Labels Sue AI Music Program Suno for Copyright Infringement

Major record labels, including Universal Music Group, Sony Music Entertainment, and Warner Music Group, have collectively filed a lawsuit against AI music program Suno AI for alleged copyright infringement. The lawsuit contends that Suno AI has exploited copyrighted sound recordings without permission, impacting artists and labels alike. The plaintiffs argue that Suno's training practices involve copying specific copyrighted recordings, as evidenced by outputs closely resembling targeted sound recordings. They emphasize the importance of upholding copyright law to incentivize creativity while allowing for technological innovation. The lawsuit seeks injunctions and damages reflecting the scale of Suno's alleged infringement.

Hong Kong regulatory released its Model Framework for AI

The Privacy Commissioner for Personal Data (PCPD) has launched a framework guiding AI development in Hong Kong under the PDPO. Endorsed by government and tech sectors, it promotes responsible AI use while enhancing data privacy. Covering governance, risk assessment, data management, and stakeholder engagement, the framework supports Hong Kong's digital economy goals and aligns with national AI initiatives.

PRIVACY DIGEST

AI System Development: CNIL’s GDPR Compliance Recommendations

The CNIL has published recommendations to help AI developers comply with GDPR, clarifying that responsible data use is crucial for innovation. These guidelines apply to AI systems using personal data and cover design, dataset creation, and model training phases. Key steps include defining the system’s purpose, establishing legal bases for data processing, minimizing data use, setting retention periods, and conducting Data Protection Impact Assessments (DPIAs). Aligned with the EU AI Act, the CNIL's advice aims to ensure data protection without stifling innovation. Upcoming how-to guides on topics like web scraping and data rights will be available for public consultation.

FINES AND PENALTIES

Italy: Garante Imposes €20,000 Fine on National Institute of Social Security for Data Breach

In a recent decision dated June 6, 2024, the Italian data protection authority, Garante, fined the National Institute of Social Security (INPS) €20,000 for unlawfully publishing personal data. This action followed a complaint regarding INPS's disclosure of sensitive information, including candidate lists and test scores, without proper authorization. Garante found INPS in breach of GDPR Articles 5 and 6, highlighting the dissemination of personal data without legal basis.

PRIVACY DIGEST

Belgium: DPA Imposes €172,431 Fine on Unnamed Company for GDPR Violations

On June 3, 2024, the Belgian Data Protection Authority (Belgian DPA) fined an unnamed company €172,431 for GDPR violations related to noncompliance with data subject rights. The decision, No. 87/2024, stemmed from a complaint about unauthorized direct marketing despite the data subject's right to erasure and objection. The Belgian DPA found the company failed to respect these rights and neglected to take appropriate measures in response. The fine reflects breaches of GDPR Articles 5(1)(a), 5(2), 17, 21, and 24.

Allianz Fined €200,000 by Spain's AEPD for Data Security Breach

The Spanish data protection authority, AEPD, has levied a fine of €200,000 against Allianz, citing violations of the General Data Protection Regulation (GDPR) following an investigation into a complaint. The AEPD discovered that an Allianz employee accessed and shared the complainant’s personal data with their former partner, highlighting failures in data integrity and confidentiality safeguards. Additionally, Allianz was found lacking in implementing adequate technical and organizational security measures. This incident underscores the importance of robust data protection practices and compliance with GDPR requirements.

PRIVACY DIGEST

DATA BREACH UPDATES

TeamViewer Detects Security Breach in Corporate IT Environment

On June 26, 2024, TeamViewer identified a security breach in its corporate IT environment. Immediate actions were taken to investigate and mitigate the issue. The attack, attributed to the Russian state-sponsored group APT29, compromised an employee account, gaining access to names, corporate contact information, and encrypted passwords.

TeamViewer confirmed that customer data and the product environment were not affected. The company has enhanced its security measures and is rebuilding its IT environment, with ongoing investigations and updates to follow.

Hackers Breach BSNL Again, Second Time in Six Months

BSNL has experienced a second data breach in six months, with hackers accessing over 278 GB of sensitive information, including international mobile subscriber identity (IMSI) numbers, SIM card details, and critical security keys. The breach, orchestrated by a threat actor named "kiberphant0m," poses significant risks, such as SIM cloning and potential extortion. The compromised data could lead to sophisticated cyber-attacks on BSNL and other interconnected systems, posing national security risks. This follows a similar breach last December, where data involving 32,000 lines of BSNL's fibre and landline users were exposed. The current breach involves distinct, more complex data related to BSNL’s telecom operations.

PRIVACY DIGEST

Truist Bank Confirms Data Breach

Truist Bank, a top 10 US bank, confirmed a data breach on June 12, 2024. A dark web broker named “Sp1d3r” offered stolen data, including 65,000 employee records, bank transactions, and IVR source code, for $1,000,000. Truist, formed by the merger of SunTrust Banks and BB&T, denied any link to a Snowflake-related breach, stating an October 2023 incident was quickly contained and affected customers were notified. Protect yourself by following vendor advice, changing passwords, enabling two-factor authentication, avoiding phishing, not storing card details online, and setting up identity monitoring.

How to Avoid a Data Breach

Avoiding a Data Breach:

Security Measures: Use firewalls, antivirus software, and encrypt data.
Updates: Regularly update software to fix vulnerabilities.
Access Control: Enforce least privilege and multi-factor authentication.
Training: Educate employees on security best practices.
Audits and Testing: Conduct security audits and penetration tests.
Backups: Regularly back up data securely.
Physical Security: Restrict physical access to sensitive data.

After a Data Breach:

Containment: Identify and contain the breach.
Damage Assessment: Evaluate the breach's impact.
Notification: Inform affected parties and stakeholders.
Legal Compliance: Report the breach as required by law.
Investigation: Determine the breach's root cause.
Remediation: Fix vulnerabilities and update policies.
Communication: Keep stakeholders informed.
Monitoring: Increase system monitoring and review security measures.

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.