Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

December 2024

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

PRIVACY DIGEST

GLOBAL DEVELOPMENTS AT A GLANCE

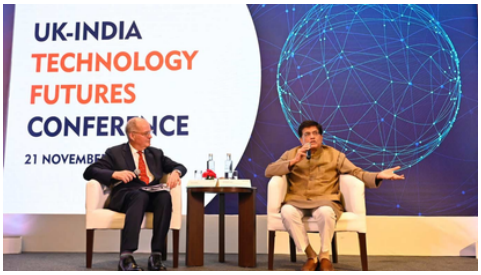
As data privacy becomes an increasingly critical issue, countries worldwide are taking bold steps to redefine how personal data is managed, protected, and shared. India is gearing up to introduce a new legal framework that balances privacy with the free flow of data across borders. Meanwhile, the EU's Cyber Resilience Act is setting new standards for cybersecurity, applying stringent rules to AI systems and digital products. In Vietnam, a new draft law aims to strengthen data privacy protections, and the US is pushing for more transparency in AI training with the TRAIN Act. With these global shifts, it's clear that the future of data protection will require adaptability and strong governance. Here's a look at how the world is evolving on this front.

PRIVACY DIGEST

ASIA PRIVACY UPDATES

India to Introduce New Legal Framework for Data Privacy and Global Data Flow

Union Minister Piyush Goyal announced India's plans for a new legal framework to ensure data privacy while facilitating the free flow of data among trusted global partners. Speaking at the UK-India Technology Futures Conference, Goyal highlighted India's capabilities in sustainable digital infrastructure, underpinned by a robust legal system and a clean energy grid set to reach 1,000 gigawatts by 2030. He emphasized sustainability concerns tied to energy-intensive data processing and proposed collaboration between India and the UK in areas like AI-based education, telemedicine, climate modeling, precision farming, and advanced industrial innovation.



India Opts for Voluntary Codes Over Direct AI Regulation

India has decided against direct AI regulation, opting instead for voluntary codes and leveraging existing laws for issues like personal data protection, fraud, and copyright concerns. The Ministry of Electronics and IT (MeitY) plans to release "informal directive principles" in early 2025, focusing on the robustness of AI systems using a risk-based approach. While there are no plans for a separate AI regulatory body, the government may establish an AI safety institute to set development standards. Meanwhile, MeitY is drafting legislation to mandate watermarks on generative AI content and exploring legal frameworks requiring large language models to train on Indian languages and local contexts.

Vietnam's Draft Personal Data Protection Law: Strengthening Data Privacy Standards

Vietnam has released the first draft of its new Personal Data Protection Law (PDPL) for public consultation, aiming to establish a robust framework for personal data privacy, effective from January 1, 2026. The draft law introduces stricter provisions compared to the previous Personal Data Protection Decree, addressing issues such as consent requirements, cross-border data transfers, data breach notifications, and compliance obligations for businesses. Key features include clearer distinctions between basic and sensitive personal data, mandatory Data Protection Impact Assessments (DPIAs), and prohibitions on personal data sales. Financial and credit institutions are also bound by stringent data security standards. While the law is expected to align with global standards, businesses will need to adapt to these changes, particularly around data processing and sensitive data protection, as the draft moves towards potential adoption in May 2025.

PRIVACY DIGEST

EU PRIVACY UPDATES

EU Adopts New Product Liability Directive Addressing AI and Digital Products

The EU's updated Directive 2024/2853 on liability for defective products took effect on November 18, 2024, replacing the 1985 directive. The revision modernizes liability rules to address challenges posed by artificial intelligence, digital technologies, circular economy models, and global supply chains. It expands the definition of "product" to include digital goods such as software, digital design documents, and AI systems. Under the new directive, developers and manufacturers of software and AI systems, as defined by the AI Regulation (EU) 2024/1689, are classified as manufacturers and can be held liable for damages caused by their systems, regardless of a contractual relationship with the claimant.

EDPB Reviews EU-U.S. Data Privacy Framework and Highlights Privacy Concerns in Law Enforcement Data Access

The European Data Protection Board (EDPB) released its first review of the EU-U.S. Data Privacy Framework (DPF) and issued a statement on recommendations for law enforcement data access. While noting progress in implementing the DPF, including certification processes and a redress mechanism, the EDPB urged U.S. authorities to strengthen monitoring of company compliance and clarify data transfer guidelines. It also emphasized the need for safeguards like proportionality in U.S. public authority data access and called for close monitoring of Section 702 of the U.S. Foreign Intelligence Surveillance Act. Addressing law enforcement, the EDPB expressed concerns over broad data retention mandates and encryption-weakening proposals, stressing the need to balance effective law enforcement with fundamental privacy rights.

UK Approves First Data Protection Code of Conduct for Private Investigators

The UK has approved and published the first sector-specific data protection code of conduct for private investigators, the ABI UK GDPR Code of Conduct for Investigative and Litigation Support Services. This code, created by the Association of British Investigators (ABI), helps ensure investigators comply with UK GDPR requirements while balancing investigative work with privacy rights. It addresses key issues like data controller roles, Data Protection Impact Assessments, and lawful processing for covert surveillance, background checks, and social media monitoring. The code aims to provide clarity and accountability for investigators, fostering transparency and best practices in data protection.

PRIVACY DIGEST

EU Cyber Resilience Act Published, Extends to AI Systems

The EU Cyber Resilience Act (CRA), published on November 21, 2024, in the Official Journal of the EU, will come into force in 20 days, establishing mandatory cybersecurity requirements for digital products and software throughout their lifecycle. Designed to ensure harmonized rules across the EU, the CRA applies to high-risk AI systems under the EU AI Act, requiring compliance with essential cybersecurity standards outlined in its Annex I. While the regulation takes full effect on December 11, 2027, certain provisions, such as Article 14, will apply earlier, starting September 11, 2026. The CRA aims to enhance security for consumers and businesses, aligning AI governance with robust cybersecurity frameworks.

DATA BREACH

HDFC Life Confirms Data Breach Amid Rising Cyber Threats in Insurance Sector

HDFC Life Insurance has reported a data breach involving the unauthorized sharing of sensitive customer information by an unknown source. The company has initiated a detailed investigation with information security experts to assess the breach's scope and take corrective measures. In response to this and other recent breaches at Star Health and Tata AIG, the Insurance Regulatory and Development Authority of India (IRDAI) has mandated IT system audits for insurers and emphasized protecting policyholder data. IRDAI is actively monitoring these incidents and working with insurers to mitigate risks and safeguard customer interests.

PRIVACY DIGEST

US PRIVACY UPDATES

Canadian Privacy Commissioners Urge Action Against Deceptive Design Patterns in Digital Platforms

During their annual meeting in Toronto, Canada's privacy commissioners and ombudsmen issued a joint resolution addressing the widespread use of deceptive design patterns, also known as "dark patterns," on websites and mobile apps. These practices manipulate users into making privacy-compromising decisions, often by using inaccessible language, obstructive design, or forced data sharing. Highlighting findings from the Global Privacy Enforcement Network's 2024 investigation, which revealed these patterns in 99% of Canadian sites examined, the commissioners urged organisations to adopt privacy-by-design principles, ensure transparency, and minimize data collection. They emphasized safeguarding children's privacy and protecting user autonomy across digital platforms.

Office of the Privacy Commissioner of Canada

Quebec Introduces New Rules for Managing and Reporting Cybersecurity Incidents

Starting April 23, 2025, the new regulation in Quebec requires financial institutions and credit reporting agents to implement an information security incident management policy and designate a responsible individual. High-risk incidents must be reported to the Autorité des marchés financiers within 24 hours, with follow-ups every three days and a final report within 30 days. Organizations must also maintain a five-year incident log. Non-compliance could result in fines of $1,000 or $2,500 per violation.

CFPB Issues Guidance on Employer Use of Digital Surveillance Tools

The Consumer Financial Protection Bureau (CFPB) has issued guidance addressing the use of digital surveillance tools by employers to monitor and evaluate employees. These tools track various activities, including sales interactions, driving habits, task completion times, communication frequency, and meeting participation. Employers utilize this data for decisions related to hiring, compensation, and overall employee management, including disciplinary actions. The CFPB emphasizes that organizations employing algorithmic tools and third-party consumer reports for employee evaluation must comply with the Fair Credit Reporting Act (FCRA).

PRIVACY DIGEST

U.S. TRAIN Act Proposes New Copyright Disclosure Rules for AI Training

On November 25, 2024, U.S. Senator Peter Welch introduced the Transparency and Responsibility for Artificial Intelligence Networks (TRAIN) Act to amend U.S. Copyright Law (Title 17). The bill allows copyright owners to request subpoenas compelling AI model developers or deployers to disclose records of copyrighted works used in training generative AI models, provided the owner has a "subjective good faith belief" of such use. Non-compliance creates a rebuttable presumption that the developer made copies of the works, though defenses like "fair use" remain available. While the legislation aims to increase transparency and assist creators, its practical impact is expected to favor collective actions more than individual litigants, raising critical questions about whether AI training constitutes copyright infringement.

California Approves New Regulations for Data Brokers to Strengthen Consumer Privacy

On November 8, 2024, the California Privacy Protection Agency (CPPA) approved new regulations for data brokers to enhance consumer privacy under the Delete Act. The regulations require data brokers to register with the state and ensure they delete personal data upon consumer request within 45 days. The rules define data broker relationships, expanding the scope to include businesses with direct consumer relations that also sell data not collected directly from consumers. The CPPA also introduced an increased registration fee of USD 6,600 and plans to implement a consumer-friendly deletion system, DROP, by 2026. Enforcement has begun, with the CPPA fining companies like Growbots and UpLead for non-compliance. These regulations are part of California's broader effort to protect personal data and hold data brokers accountable.

PRIVACY DIGEST

AI UPDATES

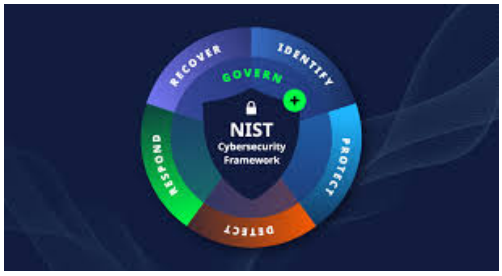
Australian Inquiry Criticizes Big Tech's Use of Data for AI Training and Urges New Laws

An Australian Senate inquiry has criticized Amazon, Google, and Meta for their lack of transparency regarding the use of Australian data in training AI models, with the inquiry chair accusing them of "pillaging culture, data, and creativity." The report recommends standalone AI legislation, mandatory transparency, and compensation mechanisms for creative workers whose content is used to train AI systems. It categorizes general-purpose AI models like GPT and Google Gemini as "high risk," calling for stringent accountability. While the Coalition members of the inquiry cautioned against stifling innovation, the Greens argued the recommendations fall short of international regulatory standards.

Spain Proposes Collective Licensing System for AI Training on Copyrighted Works

Spain has unveiled a draft Royal Decree aimed at regulating collective licenses for the mass use of copyrighted works in AI training. The decree, aligned with Article 12 of the EU Copyright Directive, proposes extended collective licenses to simplify obtaining non-exclusive authorizations for general-purpose AI model development. Key conditions include ensuring representativeness of rights management entities, equal treatment of rights holders, opt-out mechanisms for non-authorizing rights holders, and publicizing terms before use. This draft could set a precedent for other EU nations and reshape AI copyright practices across Europe.

NIST Releases Report on Mitigating Risks of AI-Generated Synthetic Content



The U.S. National Institute of Standards and Technology (NIST) has published a report titled "Reducing Risks Posed by Synthetic Content", outlining strategies to combat the risks associated with AI-generated deepfakes. The report emphasizes three key approaches: tracking content provenance to reveal its source and history, developing tools to label and identify AI-generated content, and curbing the creation and spread of AI-generated CSAM and NCII. Highlighting risks ranging from disinformation and cybersecurity breaches to individual harm through misuse, the report advocates for tailored detection and transparency techniques to mitigate these challenges.

PRIVACY DIGEST

FINES AND PENALTIES

LinkedIn Fined for Misuse of Legitimate Interests in Data Processing

At the IAPP Europe Data Protection Congress 2024, Ireland's Data Protection Commission (DPC) elaborated on its €310 million fine against LinkedIn for improper reliance on legitimate interests as a legal basis for processing personal data for targeted advertising and analytics. While LinkedIn met the first two prongs of the CJEU's three-part test—pursuing legitimate interests and demonstrating data processing necessity—it failed the third, as user rights and expectations were deemed to outweigh the company's interests. The DPC highlighted concerns about inferred data misuse, such as gender or age-based targeting or exclusion from job opportunities. Experts at the conference emphasized the complexities of balancing innovation with robust legal compliance, urging businesses to enhance legitimate interest assessments and collaborate with regulators to address rapid technological advancements.

South Korea Fines Meta $15 Million Over Data Breach

South Korea's Personal Information Protection Commission (PIPC) has fined Meta $15.67 million (21.62 billion won) for violations of the country's Personal Information Protection Act (PIPA), citing the improper sharing of sensitive data from around 980,000 users, including political, religious beliefs, and sexual orientation, with over 4,000 advertisers without explicit consent. The PIPC also criticized Meta for denying users' requests to access their personal data and for failing to secure an outdated account recovery page, which led to a data breach. This penalty highlights the increasing global trend of stricter data privacy enforcement, emphasizing that tech companies must obtain explicit consent for processing sensitive data, ensure transparency in user data access, and implement robust security measures. The ruling serves as a reminder that regulatory authorities are tightening enforcement of data privacy laws, and companies must comply with local regulations to avoid significant penalties.

PRIVACY DIGEST

Thailand Fines Company THB 7 Million for Data Protection Failures

On July 31, 2024, Thailand's PDPC fined an online trading company THB 7 million for mishandling customer data, leading to a breach where scammers misused sensitive information. The company failed to appoint a Data Protection Officer, lacked proper security measures, and delayed breach reporting. In addition to the fine, the company was ordered to improve security and train staff. This case sets a precedent for strict enforcement of Thailand's PDPA, urging businesses to comply with data protection requirements to avoid penalties.

PIPC Fines Two Universities for Cybersecurity Breaches

On November 14, 2024, the Personal Information Protection Commission (PIPC) fined Soonchunhyang University KRW 193 million and Kyungsung University KRW 42.8 million for personal data leaks caused by unpatched security vulnerabilities. Soonchunhyang's homepage was hacked, leaking over 500 individuals' data, while Kyungsung's system breach affected 2,000 students. Both universities failed to apply critical security patches since 2017 and lacked adequate protections, such as Web Application Firewalls. The PIPC ordered corrective measures, including installing intrusion prevention systems, applying patches, and encrypting personal data. This case highlights the importance of timely security updates and proper cybersecurity measures to prevent data breaches and protect personal information.

Azure Data Protection Consultants LLP

Contact us for any queries:

https://azuredpc.com/

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com

DISCLAIMER