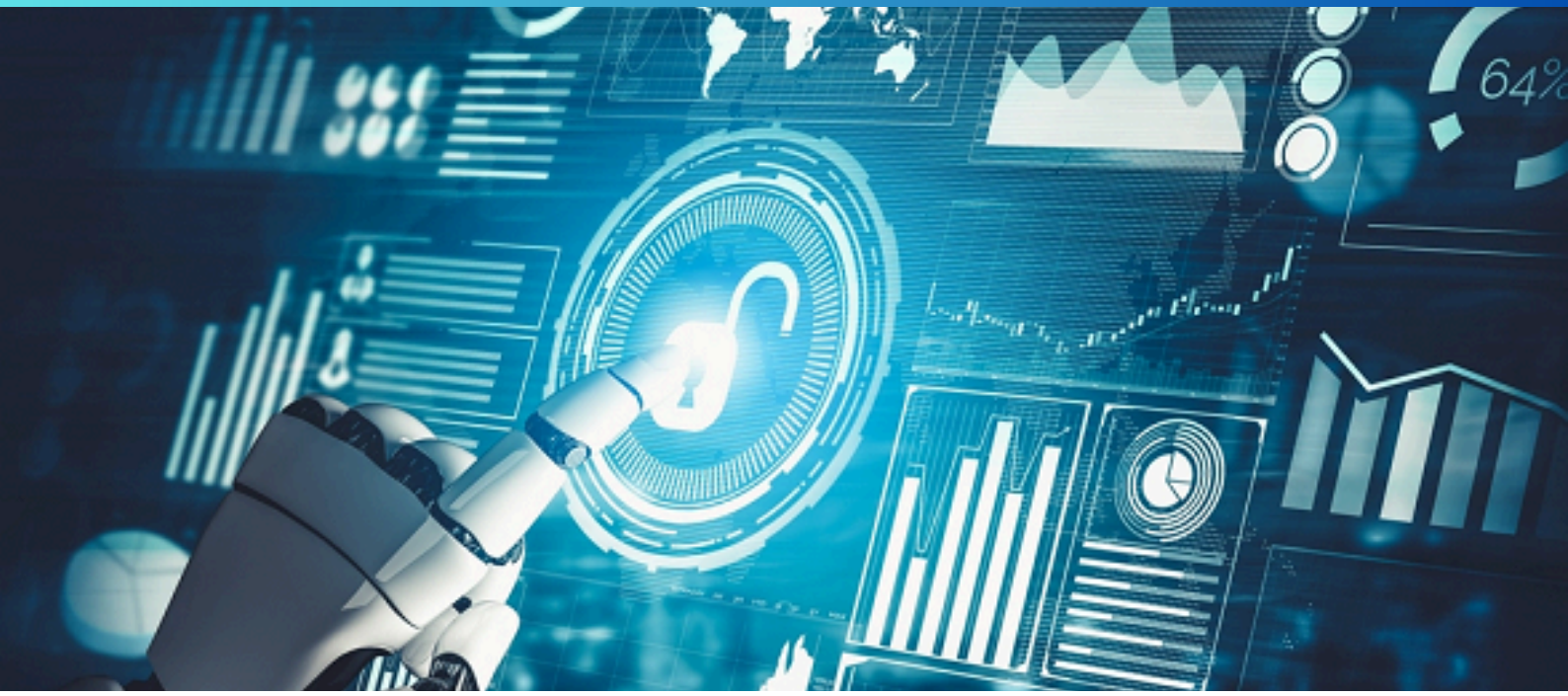
Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

February 2025

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

PRIVACY DIGEST



India's Ministry of Electronics and Information Technology has released the draft Digital Personal Data Protection (DPDPA) Rules, 2025, marking a critical step in operationalizing the Digital Personal Data Protection Act (DPDPA), 2023. These draft rules outline essential guidelines for the protection of personal data, including detailed provisions on data fiduciaries' obligations, data breach notifications, consent management, and data principal rights. The rules emphasize transparency, requiring data fiduciaries to provide clear, standalone notices detailing the categories and purposes of data processing. Additionally, they mandate immediate breach reporting, impose stricter data retention policies, and introduce unique measures like verifiable parental consent for children's data. The draft also includes a significant focus on international data transfers and establishes the role of consent managers to facilitate seamless consent processes. These rules aim to ensure compliance with global privacy standards while balancing the needs of India's diverse digital economy. As businesses and stakeholders prepare for the upcoming changes, these rules offer both opportunities and challenges for organizations to finetune their data protection strategies.

PRIVACY DIGEST

ASIA PRIVACY UPDATES

The Ministry of Electronics and Information Technology in India has unveiled the draft Digital Personal Data Protection (Act) Rules, 2025, and is open for public consultation until February 18.

India's data protection framework is undergoing a major overhaul with the Digital Personal Data Protection Act (DPDPA) 2023 and the draft Digital Personal Data Protection Rules, 2025. The draft rules, open for public consultation, detail how the DPDPA will be implemented, establishing the Data Protection Board of India as the enforcement body. While specific timelines are pending, a two-year transition period is expected for businesses. Data fiduciaries will need to provide granular, standalone notices explaining data processing purposes and categories, requiring a potential overhaul of data monetization and marketing practices, and obtaining explicit, unbundled consent. Breach reporting to the Board and affected individuals must happen "without delay," with detailed reports due within 72 hours, regardless of a materiality threshold. The rules outline data principal rights, including access, correction, and erasure, with flexible response timelines, and introduce the novel concept of nominating a representative for deceased or incapacitated individuals. International data transfer conditions will be established, potentially mirroring GDPR adequacy requirements, and significant data fiduciaries might face data localization requirements. Consent managers, as intermediaries, will facilitate consent management, data sharing, and portability, requiring Indian incorporation and adherence to strict operational guidelines. Baseline security safeguards, including encryption and access controls, are mandatory. Verifiable parental consent for children's data and due diligence for guardians of persons with disabilities are crucial. Significant data fiduciaries face additional obligations like impact assessments, audits, and algorithm verification. Large social media and e-commerce platforms must delete inactive user data after three years with prior notice. Behavioral monitoring and targeted advertising of children are generally restricted. Data processing for research, archiving, and statistics is permitted under specific conditions. The government can exempt certain data fiduciaries, possibly including news publishers and startups, from DPDPA provisions. These developments create both clarity and new compliance challenges for businesses, requiring proactive preparation for the evolving Indian data protection landscape.

सत्यमेव जयते

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

PRIVACY DIGEST

China Releases Draft Guidelines on AI-Generated Content Labeling

China's National Information Security Standardization Technical Committee (TC260) has introduced draft guidelines for labeling AIgenerated content. Open for public consultation until 5 February, these guidelines aim to standardize content labeling practices and enhance AI governance.

New Cybersecurity Guidelines for Facial Recognition Payments in China

TC260 has also issued new cybersecurity guidelines for personal data protection in facial recognition payment systems. The guidelines require payment operators, service providers, and equipment vendors to ensure secure user consent, implement multifactor verification, prevent fraud, enforce data encryption, and conduct real-time monitoring. Compliance is expected from banks, payment processors, and e-commerce platforms as digital payments continue to expand in China.

DeepSeek Launches Open-Source AI Model, Competing with OpenAI

DeepSeek has introduced its open-source AI reasoning model, DeepSeek-R1, claiming it is comparable to OpenAI's most advanced proprietary model, o1. Unlike OpenAI, DeepSeek allows its model to be used for free and freely commercialized. The company has also contributed six smaller models, based on Qwen and Llama, to the open-source community. Additionally, Alibaba Cloud has expanded its suite of large language models, including the Qwen2.5 series, offering models with parameters ranging from 7 billion to 72 billion. These models are now available to global developers via APIs on Alibaba's Model Studio platform, alongside enhanced AI tools such as Tongyi Lingma, an AI coding assistant. Alibaba Cloud also launched its 9th Generation ECS instances and the Alibaba Cloud GenAI Empowerment Program to support global innovation.

PRIVACY DIGEST

EU PRIVACY UPDATES

European General Court Upholds EDPB's Investigative Authority

On 29 January, the European General Court ruled that the European Data Protection Board (EDPB) has the authority to request a lead national supervisory authority to conduct additional investigations and issue new draft decisions. This decision came after Ireland's Data Protection Commission (DPC) challenged the EDPB's directive to further investigate Meta's data processing practices. The ruling, which can be appealed to the Court of Justice of the European Union (CJEU), strengthens the EDPB's role in GDPR enforcement.

EDPB Issues Guidelines on Pseudonymization with Consultation Open Until 28

February On 16 January 2025, the European Data Protection Board (EDPB) adopted its Guidelines 01/2025 on pseudonymization, which are now open for consultation until 28 February. The guidelines outline the legal and technical requirements for effective pseudonymization, emphasizing its importance in mitigating data privacy risks. They include 10 worked examples, including those related to medical and marketing data, and stress the necessity of keeping additional identifying information separate and secure. Notably, the guidelines discuss the implications of disclosing pseudonymized data to third parties and the potential legal risks associated with pseudonymization and its misuse.

EU Adopts European Health Data Space (EHDS) Regulation

On 21 January, the Council of the European Union adopted the European Health Data Space (EHDS), establishing a legal framework to improve individuals' access to and control over their electronic health data. The regulation enhances interoperability across EU health records and facilitates anonymized data reuse for research and innovation.

PRIVACY DIGEST

Poland's EU Council Presidency Prioritizes Digital Reforms

Starting its six-month term on 1 January, Poland's presidency of the Council of the European Union aims to reduce regulatory burdens on businesses, streamline notification obligations, and strengthen cybersecurity. It also prioritizes AI development, digital diplomacy, and international digital trade policies.

POLAND25.EU

US PRIVACY UPDATES

Trump Repeals Biden's AI Safety Order but Maintains AI Infrastructure Push

On his first day in office, President Donald Trump repealed Biden's Executive Order 14110, which had mandated AI safety testing and government oversight of high-risk AI systems. While some provisions had already been implemented, the repeal primarily affects unfinished regulatory efforts, signaling a shift away from federal AI regulation. However, Trump has not revoked Biden's Executive Order 14141, which supports AI infrastructure by leasing federal sites for private-sector AI data centers and power facilities, indicating continued focus on AI-related energy and land use. Meanwhile, regulatory shifts, including new leadership at the FTC and SEC and the appointment of an 'AI and crypto' tsar, are expected to shape AI enforcement priorities in the coming years.

New York Set to Enact Landmark Health Data Privacy Law

New York is set to enact the New York Health Information Privacy Act (NYHIPA), a stringent health data privacy law that mandates strong opt-in consent for processing health-related data, including a 24-hour waiting period for approvals. The bill, expected to be signed by Governor Kathy Hochul, could also prohibit the sale of health data. Enforcement will be led by the state attorney general, with penalties reaching $15,000 per violation or 20% of revenue from New York consumers. While potential amendments may refine its scope, NYHIPA reflects a growing trend of state-led privacy regulations in 2025.

PRIVACY DIGEST

FTC Issues Final Rule Amending COPPA to Strengthen Children's Online Privacy Protections

The U.S. Federal Trade Commission (FTC) has unanimously voted to amend the Children's Online Privacy Protection Act (COPPA) Rule, marking the first update since 2013. The revised rule, which takes effect 60 days after publication, introduces several key changes, including opt-in parental consent for the sale of children's data for targeted advertising, limits on data retention, and formalized data security requirements. The rule also clarifies the definition of personal information to include biometric and government-issued identifiers. However, provisions related to educational technology and school involvement were excluded, pending updates to the Family Educational Rights and Privacy Act (FERPA). Despite some objections from FTC commissioners, the amendments aim to enhance children's privacy protections in the digital landscape.

CFPB Issues Final Rule on Personal Financial Data Rights, Advancing Open Banking

The CFPB has issued its final Personal Financial Data Rights rule, requiring banks to share consumer financial data with designated third parties, such as fintechs, upon request, advancing open banking in the U.S. The rule includes privacy safeguards, banning data use for targeted ads, cross-selling, or resale, while mandating security measures and consumer control over data access. Large banks must comply by April 2025, with smaller entities phased in by 2030. Despite legal challenges and potential regulatory shifts under the new administration, open banking is set to transform financial services by fostering competition, innovation, and consumer financial empowerment.

PRIVACY DIGEST

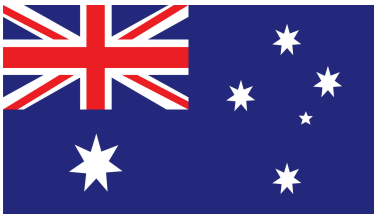
AI UPDATES

Anthropic & Universal Music Strike AI Copyright Deal

Anthropic and Universal Music Group have reached a landmark agreement following a 2023 lawsuit over AI training on copyrighted songs. Finalized on January 2, 2025, the deal requires Anthropic to enforce safeguards preventing copyright-infringing outputs. This shifts legal focus from AI training practices to output control effectiveness. If accepted by courts, it could set a precedent allowing AI training on copyrighted content under fair use, provided sufficient protections are in place. The agreement may shape future AI copyright disputes globally.

ANTHROP\C

Australia Passes Major Privacy and Cybersecurity Laws



The Australian government has enacted the Privacy and Other Legislation Amendment Bill and the Cyber Security Act, along with amendments to the Security of Critical Infrastructure Act 2018, Intelligence Services Act 2001, and Freedom of Information Act 1982. These changes aim to strengthen data protection, enhance cybersecurity measures, and improve transparency in government operations. The new laws will be implemented gradually, with regulators and businesses preparing for compliance.

Australia Funds Social Media Age Restrictions & Children's Privacy Code

Australia's OAIC will receive AUD 5 million (2024-2028) and AUD 1.1 million annually from 2028 to enforce new social media age restrictions under the Online Safety Act. Additionally, AUD 3 million (2024-2027) is allocated to develop a Children's Online Privacy Code, strengthening data protections under Privacy Act reforms.

Australian Government

Office of the Australian Information Commissioner

PRIVACY DIGEST

FINES AND PENALTIES

PayPal Fined $2M for Data Breach Exposing 35,000 Customers

PayPal will pay a $2 million fine to New York State for cybersecurity failures that led to a 2022 data breach exposing 35,000 customers' personal data. The breach was caused by weak security controls, including the lack of multi-factor authentication and improper handling of IRS Form 1099-K data. New York's DFS found PayPal violated cybersecurity policies and failed to train employees on system changes. While PayPal has since improved security measures, the fine highlights the importance of compliance, with no further action unless new violations arise.

PIPC Fines KakaoPay, Apple, and Alipay for Illegal Data Transfers

The Personal Information Protection Commission (PIPC) has imposed fines and corrective actions on KakaoPay, Apple, and Alipay for illegal overseas transfers of personal data. KakaoPay was fined 5.97 billion won, while Apple faced a 2.4 billion won fine. Alipay, which received the data, was ordered to destroy illegally obtained information. The issue arose from KakaoPay and Apple transferring 40 million users' data to Alipay without consent. PIPC emphasized the need for businesses to secure explicit user consent before transferring data overseas and stressed the responsibility of external trustees in handling personal information.

PRIVACY DIGEST

DATA BREACH

HPE Investigates Source Code Breach by IntelBroker

Hewlett Packard Enterprise (HPE) is investigating a security breach after the hacking group IntelBroker claimed to steal its source code, including sensitive credentials and product data. While no customer data was leaked and operations were unaffected, the breach exposed old user information. HPE has activated response protocols and is investigating the incident.

Tata Technologies Recovers from Ransomware Attack, Calls for Industry 4.0 Upskilling

Tata Technologies confirmed a ransomware attack that temporarily disrupted some IT services. However, all affected services have now been restored. The company is investigating the breach and ensuring data security. In related news, CEO Warren Harris emphasized the need for increased investment in upskilling for Industry 4.0 technologies, such as AI and IoT, to support India's economic growth. Tata Technologies also urged government support for innovation and infrastructure to build a future-ready workforce.

DeepSeek AI Startup Exposes Sensitive Data in Major Breach

Chinese AI firm DeepSeek accidentally exposed over 1 million sensitive records, including chat histories and API secrets, due to an unsecured database. The breach has raised concerns about AI security risks. DeepSeek secured the data quickly after being alerted, but the incident has attracted global scrutiny, with investigations underway in the U.S., Italy, and Ireland. This highlights the need for stronger security practices in AI development.

Azure Data Protection Consultants LLP

Contact us for any queries:

https://azuredpc.com/

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com

DISCLAIMER