PRIVACY DIGEST

Latest Trends

G20 announces declaration on technological transformation and digital public infrastructure

September 10, 2023

The G20 leaders met in New Delhi, under the leadership of Indian Prime Minister Narendra Modi. The G20 conference proposed several initiatives. India welcomed the commitment to support the Digital Public Infrastructure (DPI) framework. India also proposed creating a Global Digital Public Infrastructure Repository (GDPIR), a virtual repository of DPI shared by G20 members and introduced One Future Alliance (OFA), a voluntary initiative to build capacity, provide technical assistance, and support funding for implementing DPI in Low and Middle-Income Countries (LMICs). India welcomed the G20 Toolkit on Cyber Education and Cyber Awareness of Children and Youth.

The need for monitoring the crypto ecosystem and endorsing Financial Stability Board's (FSB) high-level recommendations for regulating crypto-assets and global stablecoin arrangements was emphasized. India affirmed its commitment to G20 AI Principles (2019) and called for international cooperation and discussions on global governance for AI. Additionally, India is committed to responsible AI development, addressing human rights, transparency, fairness, ethics, privacy, and data protection.

PRIVACY DIGEST

India Establishes Its Comprehensive Data Protection Law

August 11, 2023- India has successfully enacted its data protection legislation, known as the 'Digital Personal Data Protection Act, 2023'. This law received approval from both Houses of the Parliament. Following that, it received the President's Assent on August 11, 2023, and was published in the Official Gazette. Here are the main focal points of the act:

Some of the essential highlights:

Transition Period: The specific duration has not been finalized, it is expected to be around six months, ensuring an orderly transition.

Data Protection Board (DPB): Government revealed that they are prepared to notify the DPB soon. This body will play a crucial role in overseeing data protection and managing complaints under the Digital Personal Data Protection (DPDP) Act.

Awareness and Adjustment: The government aims to provide ample time for people to understand their rights under the Act. Additionally, small and medium-sized enterprises (MSMEs) will be given time to adjust to the new rules.

Appointment of DPB: Once the DPB is notified, the process of appointing its members is expected to take approximately one month.

Import Restrictions: Chandrasekhar clarified that there are no plans to extend the deadline for import restrictions on IT hardware, which is set to commence on November 1. These measures are aimed at ensuring the sourcing of IT hardware from trusted suppliers.

September 2023

AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

Key Highlights of the Digital Personal Data Protection Act, 2023

1 APPLICABILITY

The DPDP Act focuses on regulating the processing of personal data collected in digital form or digitized subsequently. It applies extraterritorially to digital personal data processed outside India if linked to offering goods or services to Indian data principals. The Act excludes personal data processed by individuals for personal purposes or publicly available data.

2 CONSENT & NOTICE

Consent is pivotal for processing personal data, requiring it to be free, specific, informed, unconditional, and unambiguous. Consent should be obtained through clear affirmative actions, and individuals can withdraw it as easily as they provide it. A notice must precede or accompany consent requests, detailing data processing purposes and rights to withdraw consent and make complaints. Consent notices should be available in various languages.

3 LEGITIMATE USES

The concept of legitimate uses enables data fiduciaries to process personal data without consent in certain cases. These cases include where the data has been willingly shared, when processing is vital for state-provided services or advantages when compliance with laws or judgments is essential when addressing medical emergencies or delivering medical care, when linked to employment objectives, or when necessary to uphold public safety and welfare.

4 OBLIGATIONS OF DATA FIDUCIARY

Data fiduciaries are accountable for compliance with the DPDP Act, even when data processing is carried out by processors on their behalf. When personal data influence decisions affecting data principles or is shared with other fiduciaries, accuracy, and completeness must be ensured. Data fiduciaries must delete personal data upon consent withdrawal or when its purpose is fulfilled, except when retention is legally mandated.

PRIVACY DIGEST

5 CROSS-BORDER DATA TRANSFER

Under the DPDP Act, the government will create a blacklist of countries. Personal data can be freely transferred unless the Central Government blacklists the destination country. If there are other laws or sectoral regulations providing higher data protection or transfer restrictions, they will take precedence.

6 RIGHTS OF DATA PRINCIPAL

Data principals possess the right to access summaries of their processed personal data and related activities. They can request corrections, updates, and erasure of personal data if no longer needed. Grievance mechanisms must be provided, with the option to escalate to regulatory boards. Data principals can nominate representatives to exercise their rights in the event of their death or incapacity.

7 DATA PROTECTION BOARD OF INDIA

The DPDP Act proposes establishing a Data Protection Board (DPB) for enforcement purposes. The DPB has the authority to address personal data breaches, conduct inquiries, impose penalties, inspect documents, and compel attendance.

8 EXEMPTIONS

The rights of Data Principals and the responsibilities of Data Fiduciaries regarding data security may be exempted in specific cases. These situations consist of instances such as preventing and investigating offenses, as well as enforcing legal rights or claims. The Central Government holds the ability to exclude specific activities from these requirements through official notifications. Such activities encompass data processing by government entities for reasons of state security and public order, along with activities related to research, archiving, or statistical purposes.

9 PENALTIES

Monetary penalties, ranging up to INR 250 crores, can be imposed by the DPB based on the breach's nature, severity, duration, data type, repetition, and more.

PRIVACY DIGEST

PETs research bill clears US House committee

August 1,2023

The U.S. House Committee on Science, Space and Technology voted 35-0 on a favorable report for House Resolution 4755 on privacy-enhancing technology research. The bill, which is now eligible for full House consideration, aims to support research on privacy enhancing technologies and promote responsible data use.

Israel:

• August 3, 2023- Israel PPA publishes draft guidance for collection of employee biometric data. The document titled "Policy Paper: Collection and Use of Biometric Data at the Workplace" recommends employers avoid collecting biometric data but allows some instances of biometric monitoring of employees during work hours.

• August 6, 2023- Israel's PPA publishes right of access guidance. The PPA sought to clarify obligations for the right to access in instances of exempted "databases of security authorities and other authorities defined by the law.

• August 10, 2023- Israel PPA releases guidance for data transfers to EEA. The instructions contain four main requirements, including the obligations to delete personal information, to limit the retention of unnecessary information and to be accurate.

South Korea's PIPC offers guidelines on personal data for AI

August 3, 2023

South Korea's Personal Information Protection Commission published guidance on using personal data to support artificial intelligence technologies. The guidelines outline principles for processing personal information in stages of AI, providing prompt legal interpretation and consulting support. The PIPC said the guidance reflects current regulation under existing privacy law while also providing "a blueprint for the government and the private sector to jointly design a regulatory system in the future.

PRIVACY DIGEST

China

• August 3, 2023- CAC published draft rules requiring service providers that maintain data on more than 1 million people to perform annual compliance audits. These reviews, to be conducted by a CAC-appointed agency, must also evaluate services with data of more than 100,000 users or sensitive data of more than 10,000 users. The CAC said services with data of less than 1 million users should undergo a personal information compliance check at least biennially.

• August 8, 2023- CAC publishes draft facial recognition rules. The draft rules include provisions for purpose limitation, necessity, required consent and prohibitions on where the technology can be installed. The CAC advised alternatives to facial recognition or other biometric identifiers should be considered before any rollout.

• August 9, 2023- National Information Security Standardization Technical Committee seeks comments on draft cybersecurity national standard for the Handling of Sensitive Personal Information. The draft defines categories of sensitive personal information, data identification and security requirements for processing, while noting the data should be processed for a specific purpose and with individual's consent. The deadline for comments is 8 Oct.

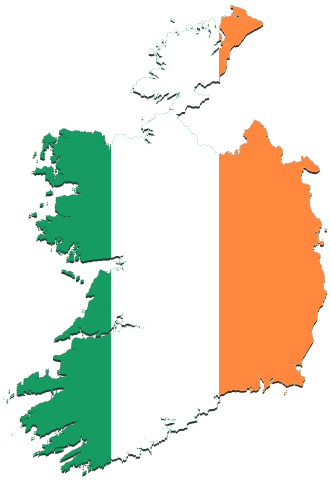
Saudi Arabia's new Personal Data Protection Law (PDPL) comes into effect

September 14, 2023

The Implementing Regulations for the PDPL and for Personal Data Transfer outside the Kingdom were published last week by SDAIA and the NDMO and provide clarity on the measures that organizations will be required to implement to ensure with the PDPL before the end of the 1-year grace period.The Implementing Regulations and the Personal Data Transfer Regulations both expand on the general principles and obligations outlined in the PDPL.

PRIVACY DIGEST

Irish Data Protection Commission announces €345 million fine of TikTok



September 15, 2023

Irish Data Protection Commission announces €345 million fine of TikTok wherein its binding decision, the EDPB analyzed the design practices implemented by TikTok in the context of two pop-up notifications that were shown to children aged 13-17: the Registration Pop-Up and the Video Posting Pop-Up. The analysis found that both pop-ups failed to present options to the user in an objective and neutral way. The EDPB also found that, as a result of the practices in question, TikTok infringed the principle of fairness under the GDPR.

CNIL issues parental control standards for internet access

August 1, 2023

France's data protection authority, the Commission nationale de l'informatique et des libertés, issued decisions regarding parental control standards for internet access. The first decision mandates minimum features that prohibit children under age 13 from downloading applications and blocking access to content on certain terminals. The second decision requires the mandatory features added to devices should not lead to additional data collection of children.

CCS offers mobile app privacy recommendations

August 4, 2023

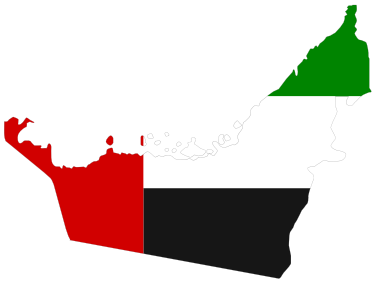
The Canadian Centre for Cyber Security released guidance to individuals and organizations for the protection of personal data when utilizing mobile apps. Recommended practices for organizations included controlling app permissions, multifactor authentication and conducting privacy setting audits.

PRIVACY DIGEST

NIST publishes draft Cybersecurity Framework 2.0

August 8, 2023

The U.S. National Institute of Standards and Technology released a public draft of its Cybersecurity Framework 2.0. The agency is seeking feedback on whether the draft addresses organizations' current and anticipated future cybersecurity challenges, is aligned with leading practices and guidance resources, and reflects comments received so far. The deadline for comments is 4 November.

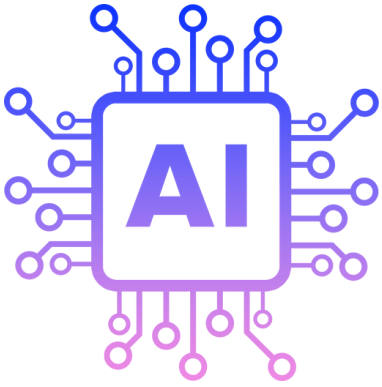


DIFC announces adequacy with CCPA

August 9, 2023

The Dubai International Financial Centre announced an adequacy decision concerning essential equivalence between the California Consumer Privacy Act and Dubai's Data Protection Law 2020. This will facilitate personal data transfers between DIFC and California-based entities in accordance with the DP Law 2020 while protecting consumers.

Canada publishes generative AI code of practice



August 16, 2023

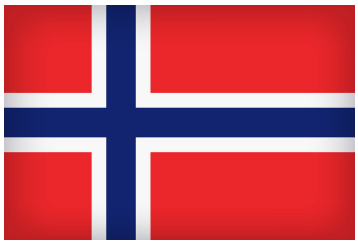
The Government of Canada published a code of practice for generative artificial intelligence development and use. In anticipation of lawmakers passing the proposed Artificial Intelligence and Data Act, the government's voluntary code will help potential covered entities avoid harmful impacts, build trust in their systems, and transition smoothly to compliance with Canada's forthcoming regulatory regime. The code includes principles for safety, fairness, transparency and human oversight.

PRIVACY DIGEST

South Korea rolls out data portability strategy

August 18, 2023

South Korea's Personal Information Protection Commission and South Korean ministries jointly announced a "paradigm shift" toward data portability throughout the digital economy. The "National My Data Innovation Promotion Strategy" initiative will empower data subjects to "realize the right to self-determination of (their) personal information" via the amended Personal Information Protection Act.



Norway DPA releases employee monitoring guidance

August 25, 2023

Norway's data protection authority, Datatilsynet, offered guidelines for monitoring employees via company-issued electronic equipment. The DPA explained how digital work tools can record large amounts of information about employees. The guidance will help employers assess what may be legal to introduce in the workplace, and give employees guidance on their rights.

Digital Services Act enforcement begins

August 25, 2023

EU Digital Services Act regulations governing the obligations of "very large online platforms" and "very large online search engines" are in effect. Platforms and search engines with more than 45 million active EU users must now submit risk assessments to the European Commission. The full DSA for smaller websites goes into effect in early 2024.

PRIVACY DIGEST

NIST issues draft cybersecurity and privacy learning program guidance

August 28, 2023

The U.S. National Institute of Standards and Technology published its initial draft of the government's cybersecurity and privacy learning program. The document offers recommendations for initiatives, such as integrating privacy with cybersecurity in organization-wide learning programs and creating a data life cycle model allowing for ongoing, iterative improvements and changes to accommodate cybersecurity (and) privacy. The consultation period is open until 27 Oct.

ICO publishes guidance on email communications

August 30, 2023

ICO also published guidance for organizations on protecting personal information when sending bulk emails. Organisations that use and share large amounts of data, including sensitive personal information, should consider using other secure means to send communications, such as bulk email services, so information is not shared with people by mistake. ICO warned organizations against using the blind carbon copy function when sending emails containing sensitive personal information.

Jordan approves draft personal data protection law

August 30, 2023

Jordan's Parliament announced its House of Representatives approved the amended draft Protection of Personal Data law. Amendments approved by the House allow the entities subject to the control and supervision of the Central Bank to process personal data, including transferring and exchanging data inside or outside the Kingdom, without informing the natural person whose data is being processed.

PRIVACY DIGEST

Switzerland DPA releases data protection impact assessment guide

August 31, 2023

Switzerland's Federal Data Protection and Information Commissioner, published an information sheet for conducting data protection impact assessments. Following the passage of the revised Data Protection Act, the document instructs federal bodies and citizens to prepare a data protection impact assessment if the planned data processing entails a high risk for the (personal data) or the fundamental rights of the persons concerned.

Data Breaches

17 hospitals in South Korea suffers data leak

August 1, 2023

South Korea's Personal Information Protection Commission found 17 hospitals exposed personal medical information of more than 185,000 patients. The hospitals were issued fines totaling KRW64.8 million for violating the Personal Information Protection Act.

Northern Ireland police leaked information of 1000s of officers

August 8, 2023

The Police Service of Northern Ireland inadvertently leaked the names, locations and ranks of 10,000 officers and civilian personnel in response to a Freedom of Information request.

1.5M individuals suffers data breach by data breach at Alberta Dental Service Corporation

PRIVACY DIGEST

1.5M individuals suffers data breach by data breach at Alberta Dental Service Corporation

August 10, 2023

Public dental benefits administrator Alberta Dental Service Corp. announced a data breach affecting approximately 1.47 million individuals. Ransomware attack of the government-backed ADSC involved access to names, addresses and personal banking information of at least 7,300 individuals. The system vulnerability spanned 7 May-9 July, according to ADSC, which said hackers "accessed and copied certain data from our network before deploying the malware.

Millions affected by multistate health data breach

August 14, 2023

A sensitive health data breach through hacks of file transfer service MOVEit affected at least three U.S. states. Hackers accessed its database of 4.1 million individuals while third-party data management firm PH Tech confirmed 1.7 million Oregonians had their information exposed through MOVEit. Missouri's Department of Social Services reported the same cyberattack affected an unknown number of residents.

Ontario liquor board suffers data breach

August 16, 2023

The LCBO's subscriber database for its promotional emails, which included names and email addresses, was accessed by hackers 9 Aug. The number of affected individuals was not disclosed. The incident follows a January cyberattack that locked up the LCBO's website control while hackers mined data.

PRIVACY DIGEST

Hackers unlawfully accessing and selling US credit header data

August 22, 2023

Hackers are allegedly purchasing former law enforcement identities to enter credit reporting companies' databases and then selling lifted information to fellow criminals. Credit header data includes various personal details about individuals connected to credit, but it also facilitates connections to information belonging to relatives.

US food delivery service breach affects 1.2M

August 28, 2023

U.S. food delivery service PurFoods disclosed a data breach that potentially affected personal, financial and medical data belonging to more than 1.2 million customers.

Hackers generate fake Signal app for surveillance

August 30, 2023

Hackers posted the fake app to Google Play and Samsung's Galaxy Store for download with the intention of spying on users' communications on the real Signal app. Google Play has since removed the imposter.

Fines US FCC proposes fines against telecom service providers

August 1,2023

The U.S. Federal Communications Commission announced a proposed USD20 million fine against affiliated telecommunications providers Q Link Wireless and Hello Mobile Telecom over alleged unauthorized access and disclosure of customer data. The FCC Privacy and Data Protection Task Force investigation found alleged data security issues led to access to customer proprietary network information through unauthenticated customer identities.

Azure Data Protection Consultants LLP

Contact us for any queries:

http://www.azuredpc.com

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com