



AZURE DATA PROTECTION CONSULTANTS LLP

August 2023

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

PRIVACY DIGEST



Latest Trends

India's proposed Digital Personal Data Protection Bill introduced in Parliament



August 3, 2023- India's new (5th and hopefully last) version of data protection law (DPDPB), 2023 was tabled in Lok Sabha. The draft law applies within India to the processing of personal data collecting either in digital form or any non digital form but digitized subsequently. It is also applicable to digital personal data processed outside India if the processing is in connection with offering of goods or services to data principals in India.

The draft law does not apply to state instrumentalities that the government may specify for public order, security and similar purposes. The government may also exempt startups from notice, accuracy and erasure requirements, significant data fiduciary obligation, and the obligation to complete data principal's access requests. Other exemptions include processing by individual for domestic and personal purpose, processing of personal data made publicly available by the data principals or under legal obligation, or processing that is necessary for research, archiving, statistical purposes, or if the data is not used to take decisions specific to a data principal, and processing complies with government prescribed standards. The proposed Data Protection Board will have enforcement power over DPDPB noncompliance and data breaches. Companies that are unable to protect against breaches and fulfill required breach reporting obligations would see a fine between RS50-RS250 crore. This is a welcome step in the right direction. Reach out to us, we can help you in your data protection compliance preparedness.

EC Introduces Data Privacy Framework (DPF) for Personal Data Transfers from EEA to US



July 10, 2023- The European Commission introduced the Data Privacy Framework (DPF) on July 10, 2023, as an "adequacy decision" to enable personal data transfers from the EEA to specific U.S. entities. The DPF Principles are akin to the previous Privacy Shield principles and cover notice requirements, opt-out options for individuals, accountability for onward transfers, security measures, data integrity, individual data access, and a compliance and grievance mechanism. U.S. organizations seeking self-certification must be under FTC or Department of Transportation jurisdiction, while others may need alternative data transfer methods like SCCs or BCRs.

LATEST TRENDS

PRIVACY DIGEST

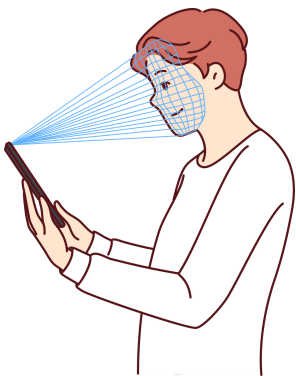


New Law Proposed to Improve Cross-Border Collaboration on GDPR Enforcement

July 5, 2023- In cross-border matters concerning the General Data Protection law (GDPR), the Commission has proposed a new law to enhance collaboration between data protection authorities (DPAs). To avoid conflicts and promote consensus, the law specifies clear procedural standards that include sharing significant issue summaries with other DPAs early during the investigation. It outlines complainants' rights, guarantees their participation, and gives parties, under investigation, the right to be heard at key stages. The idea intends to increase efficiency and collaboration among DPAs in enforcing the GDPR, expedite investigations, provide quick relief for individuals, and speed up individual remedies.

Guatemala Transparency Commission Backs Personal Data Protection Bill for Deliberation in Congress

July 6, 2023- On April 28, 2023, the President of the Transparency and Probity Commission expressed support for Bill No. 6105 of June 23, 2022, designed to enact the Personal Data Protection Law. The proposed legislation seeks to establish key data protection principles, including transparency, fairness, and confidentiality, and outlines lawful bases for data processing. It also provides a clear definition of sensitive data, protects data subject rights, and sets specific obligations for data controllers and processors. The bill is now set for further deliberation in Congress.



Montana Enacts Facial Recognition Bill for 'Serious Crimes' with Stringent Limitations

July 7, 2023- Montana has passed a new bill allowing state and local agencies, including law enforcement, to use facial recognition for identifying suspects, victims, or witnesses in "serious crimes," with certain limitations. The law prohibits continuous or real-time facial recognition, requiring human review and audits for responsible use. Law enforcement must obtain a warrant except in emergencies. Third-party vendors must inform individuals about data collection and obtain consent. Negligent violations can result in fines. The Act is effectively immediately, with existing contract arrangements having until January 1, 2024 to comply with the new requirements.

Argentina Presents Draft Personal Data Protection Bill to Chamber of Deputies

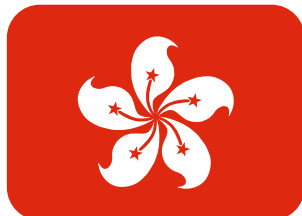
July 3, 2023- A draft Personal Data Protection Bill has been presented to the Honourable Chamber of Deputies of the Nation by Argentina's data protection body, known as the Agency of Access to Public Information. The present Personal Data Protection Act 25.326 is intended to be modified by the proposed law. The proposal contains provisions aimed at streamlining transnational data flows, enhancing children's privacy rights and data subject rights, giving data controllers additional obligations, and bringing about other pertinent improvements.



PRIVACY DIGEST



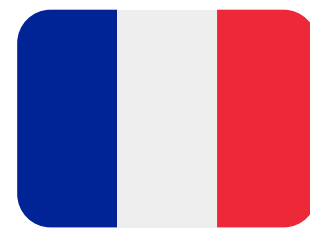
Hong Kong PCPD Releases Guidance on Data Breach Notification and Data Breach Handling



July 11, 2023- To assist organizations in effectively handling data breaches, the PCPD issued a new "Guidance on Data Breach Handling and Data Breach Notifications." This guidance presents practical recommendations and a step-by-step approach to promptly manage data breaches, minimizing harm to individuals and potential damage to organizations. The essential steps include gathering immediate information, containing the breach, assessing risks, considering data breach notifications, and ensuring proper documentation. Additionally, the PCPD introduced an e-Data Breach Notification Form to simplify the comprehensive and convenient reporting of data breach incidents.

French Data Protection Authority CNIL Issues New API Recommendation for Secure Data Sharing

July 11, 2023- The French data protection authority, CNIL, has observed a rise in data-sharing methods utilizing APIs among different entities. While APIs offer advantages in safeguarding personal data, their development, implementation, and use necessitate adherence to best practices. To promote API usage, CNIL issued a new recommendation encompassing all types of personal data sharing, organizations (public and private), and open or restricted APIs. The recommendation establishes criteria for API use and identifies risk factors for analysis, classifying three actor categories: data holders, API managers, and data reusers.



Spanish Agency for Data Protection Updates Cookie Guide to Comply with CEPD Directive

July 12, 2023- To comply with CEPD Directive 03/2022 on deceptive patterns, the Spanish Agency for Data Protection (AEPD) updated its Cookie Guide. The revised version provides concrete examples and the CEPD's criterion for prominent and equally accessible actions for accepting or rejecting cookies. Changes were made in relation to personalisation cookies, distinguishing editorial, and user consent. Furthermore, acceptance of cookies cannot be a requirement for using services, and the alternative might not be free. By January 11, 2024, these requirements must be in place, with a six-month transitional time for modifications.

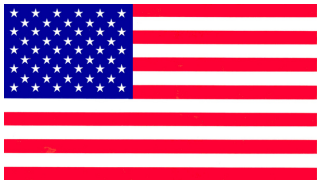


Biden Administration Unveils 'U.S. Cyber Trust Mark' to Enhance Smart Device Cybersecurity

July 13, 2023- The Biden administration revealed the forthcoming "U.S. Cyber Trust Mark" initiative, aimed at bolstering cybersecurity in smart devices. Expected to commence in 2024, the program will feature a logo on products that adhere to specific criteria set by the National Institute of Standards and Technology. Notably, numerous prominent electronics, appliance, and consumer product manufacturers, as well as retailers and trade associations, have voluntarily pledged to enhance cybersecurity measures for their offerings.



PRIVACY DIGEST



Colorado Privacy Act Comes into Force

July 13, 2023- Colorado Attorney General Phil Weiser has informed businesses that enforcement of the Colorado Privacy Act, effective since 1 July, will commence. He emphasized the significance of safeguarding consumers' data and privacy through this measure.

US Lawmakers Act Swiftly to Close Loophole in Federal Law Allowing Warrantless Data Collection

July 13, 2023- US lawmakers are moving quickly to close a federal law loophole exploited by police and intelligence agencies for collecting sensitive information on citizens without warrants. The "Fourth Amendment Is Not For Sale Act" seeks to limit purchases of Americans' data without proper legal authorization. Enjoying bipartisan support, the bill covers data acquired through hacking or company disclosures. Concerns about domestic surveillance are widespread, with related discussions also occurring regarding data purchases by the US military.

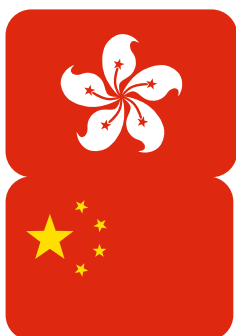
U.S. Senate Advances Critical Bills for Children's Online Safety



July 28, 2023- The U.S. Senate Committee on Commerce has advanced two bipartisan bills aimed at bolstering online safety for children, which were recently endorsed by President Joe Biden. The first bill, Kids Online Safety Act (KOSA), seeks to equip parents with tools to protect their children online and holds tech companies responsible for minors' welfare. The second bill, Children and Teens' Online Privacy Protection Act (COPPA 2.0), extends protection to children up to 16 and prohibits targeted advertising to minors.

EU and 20 Latin American and Caribbean Nations Establish EU-LAC Digital Alliance

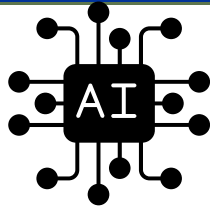
July 28, 2023- The European Union (EU) and 20 Latin American and Caribbean (LAC) countries have joined hands to create the EU-LAC Digital Alliance, a flexible platform for digital cooperation. Open to government agencies, private entities, and research networks, the Alliance strives to enhance dialogue and collaboration on a wide range of digital matters. The initiative focuses on areas such as data governance, cybersecurity, AI, digital trade, and space-related activities.



Hong Kong and China Sign MOU to Boost Cross-Border Data Flows in Greater Bay Area

July 3, 2023- The Innovation, Technology, and Industry Bureau of Hong Kong has entered a memorandum of understanding (MOU) with the Cyberspace Administration of China (CAC) with the aim of enhancing cross-border data flows in the Guangdong-Hong Kong-Macao Greater Bay Area. As per the MOU, the bureau, along with the Office of the Government Chief Information Officer and the CAC, will collaborate to investigate and implement effective management measures to promote the smooth exchange of data across the bay area.

PRIVACY DIGEST

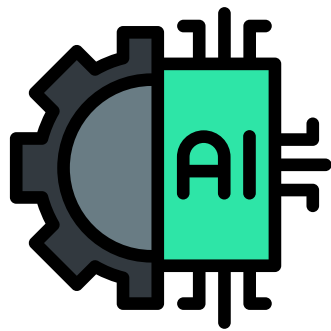


Artificial Intelligence

Argentina's Sub secretariat Releases

Comprehensive AI Guidelines for Public Sector

July 5, 2023- Argentina's Information Technology Subsecretariat issued Resolution 2/2023, presenting a comprehensive set of recommendations to promote trustworthy AI adoption within the public sector. These guidelines focus on upholding ethical principles, safeguarding fundamental rights, and prioritizing people-centric design in AI initiatives. Covering the entire AI life cycle, including design, data modelling, verification/validation, implementation, and operation/maintenance, the recommendations stress the significance of interdisciplinary teams, pre-mortem analysis, and ethical commitment to AI projects.



MIT Researchers Introduce PAC Privacy: Minimizing Noise, Enhancing Data Protection in Machine Learning

July 14, 2023- Researchers at MIT have developed a technique to protect sensitive data with minimal interference. They developed the Probably Approximately Correct (PAC) Privacy metric, which predicts the necessary noise level without needing to know the inner workings of the model. Using substantially less noise required than previous methods, PAC Privacy ensures accurate machine learning models using hidden training data in practical settings. The method makes use of the unpredictability of sensitive data and has the potential to provide secure data processing without the need for artificial alterations.

OneTrust Introduces AI Governance Solution to Ensure Responsible Use of Artificial Intelligence

July 14, 2023- OneTrust, a trust intelligence vendor, has launched its AI Governance solution to aid organizations in managing the use of their AI systems responsibly. The platform helps with data inventory work, risk assessment, and compliance with data protection laws and forthcoming AI regulations. By integrating various AI governance frameworks, the solution adapts to different AI systems and ensures human operators maintain control over the algorithms. The goal is to create a central inventory of machine learning systems and synchronize models to prevent biases and accuracy issues. With growing concerns about AI's impact, responsible AI governance becomes a crucial and labour-intensive task that requires human judgment.



Canadian Government Issues Cybersecurity Guidelines for Generative AI Use

July 21, 2023- The Canadian government has published cybersecurity recommendations for the use of generative AI. Healthcare and software development, and potential risks associated with the technology are all covered in the document. Additionally, the government has offered advice to businesses and individuals on how to reduce risk exposure while using generative AI.



PRIVACY DIGEST



Artificial Intelligence

China's AI Governance: "Interim Measures for the Management of Generative AI Services" taking effect

July 1, 2023- Cyberspace Administration of China (CAC) has finalized the 'Interim Measures for the Management of Generative Artificial Intelligence Services' that will come into effect on August 15. According to Article 2 these are only applicable to services accessible to the general public within China. If the generative AI tools are aimed at Chinese residents, offshore providers must also comply with the set of rules. It excludes generative AI services developed and utilized by enterprises, research and academic institutions, and other public entities from their scope. Technologies targeting users outside China are also exempted.



PRIVACY DIGEST



Data Breaches

Healthcare provider suffers data breach affecting 11M people.

July 10, 2023- Multinational health care provider HCA Healthcare announced it sustained a data breach affecting more than 11 million patients in the U.K. and U.S. The list of more than 27 million lines of data reportedly contained information used in emails to patients and appointment reminders. HCA officials said the data contains personally identifiable information but does not feature clinical or payment data.



Employment training agency suffers data breach, Client data exposed

July 10, 2023- Prince Edward Island's employment training agency SkillsPEI confirms data of 5,600 clients have been exposed in a breach. The agency confirmed personally identifiable information was exposed via an email sent to a recipient outside the government network. The breach was identified on 13 June and risk to client information was contained within the first 48 hours.

Chinese hackers hijacked EU and US government mails

July 12, 2023 - As per various media reports, Hackers in China reportedly exploited a Microsoft Outlook flaw and stole emails from U.S. government agencies and more than 25 European governments. The threat actor allegedly "used forged authentication tokens" to access the email accounts.



Immigration Directorate suffers data breach, 34M passport data exposed in Indonesia.

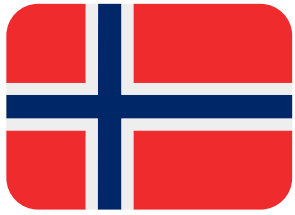
July 13, 2023- A hacker reportedly stole the passport data of 34 million Indonesian citizens. The massive data breach impacted the country's Immigration Directorate General at the Ministry of Law and Human Rights. Indonesian authorities are investigating the breach while the threat actor has offered the treasure trove for sale on his data leak site.

Canadian and US users of dating app had personal information left exposed.

July 17, 2023- Data for more than 260,000 dating app accounts and 340GB of images and private chats were left exposed in an Amazon Web Services S3 storage bucket. Canadian and U.S. users of the 419 Dating and Chat app from Siling App were the most affected and users' email addresses were also exposed.



PRIVACY DIGEST

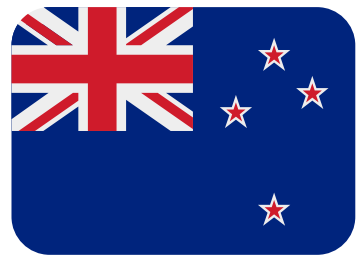


Breach compromises Norwegian government ministries

July 25, 2023- Norway's Security and Service Organization said a "data attack" compromised 12 Norwegian government ministries. Hackers exploited a software vulnerability of supplier Ivanti Endpoint Manager Mobile. The company immediately developed and released a patch and are actively engaging with customers to help them apply the fix.

New Zealand firearms license holders' email addresses leaked.

July 26, 2023- The newly established New Zealand Firearms Safety Authority inadvertently leaked information on 147 firearms license holders in Auckland. The email addresses of the license holders were revealed to each other after an email from the agency was sent with the recipients' addresses copied into the carbon copy field instead of the blind carbon copy field.



PRIVACY DIGEST



Fines and Penalties



US FTC finalizes USD7.8M fine against BetterHelp

July 13, 2023- US FTC finalized a USD7.8 million order against BetterHelp over alleged improper data sharing for advertising purposes. The order prohibits the online counseling service from sharing consumers' health data for advertising and sharing personal data for retargeting. It also requires BetterHelp to obtain affirmative express consent before disclosing personal data to certain third parties for any reason and implement a data retention schedule and comprehensive privacy program that includes strong safeguards to protect consumer data.

Payroll processing company agrees to \$6M settlement in a class action lawsuit.

July 18, 2023- Payroll processing company UKG agreed to a USD6 million settlement in multiple class-action lawsuits stemming from a 2021 ransomware attack. The attack "disrupted" the company's Kronos Privacy Cloud service, and affected entities, including Tesla, PepsiCo, and the New York Metropolitan Transport Authority. The preliminary agreement would entitle class members to USD1,000 in damages.



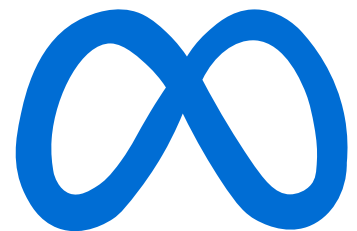
Amazon agrees to a \$25M settlement over children's privacy violations.



July 19, 2023- The U.S. Department of Justice and the Federal Trade Commission announced Amazon agreed to a permanent injunction and USD25 million civil penalty to settle alleged children's privacy violations related to its Alexa voice assistant. The complaint alleged that Amazon retained children's voice recordings indefinitely and engaged in unfair privacy practices regarding geolocation information and voice recordings. Among the requirements of the order, Amazon must identify and delete inactive child profiles.

Meta fined 20M\$ for misleading data use in Australia

July 26, 2023- Australia's Federal Court ordered Meta's Facebook Israel and the now discontinued Onavo to pay a combined AUD20 million for failing to adequately disclose data collection practices. The Australian Competition and Consumer Commission, which brought the case forward, said Meta used anonymized and aggregated data, including users' internet and app activity, for market research activities.





Azure Data Protection Consultants LLP

Contact us for any queries:



<http://www.azuredpc.com>



Azure Data Protection Consultants LLP



+91- 9599706305

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.