Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

May 2024

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

MAY 2024

AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

Latest Trends

GOVERNMENT SET TO STRENGTHEN DATA PRIVACY LAWS WITH DPDP ACT AMENDMENTS

After winning the election for the third time, the central government plans to amend the Digital Personal Data Protection (DPDP) Act and IT rules within the first 100 days of its new term. The DPDP Act's rules, pending for a long time, will strengthen the data privacy law, which is already eight months old. The amendment in IT rules will help tackle misinformation and deepfakes through artificial intelligence (AI). This move is seen as a step towards empowering the government until the comprehensive Digital India Act is enforced. Industry stakeholders have expressed concerns about the delay in notifying the rules, stating that platforms will need time to align their products and services accordingly. The amendment to the IT Rules, 2020, will focus on AI to address risks and customer damages. The Digital India Act will replace the 23-year-old Information Technology Act and will focus on cybersecurity, AI, privacy, and other related issues.

MAY 2024 AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

Privacy Protection Evolves: Exploring the Latest in Privacy-Enhancing Technologies

Privacy-enhancing technologies (PETs) enable secure data gathering, processing, and exchange while preserving privacy. These technologies, including data obfuscation, encrypted processing, federated analytics, and data accountability tools, offer efficient data use and reduce the need for extensive data collection. However, advancements in connectivity and computation have changed data processing.

Data Obfuscation: Tools like zero-knowledge proofs and differential privacy enhance privacy by altering data, adding noise, or removing identifying details. Careful implementation is crucial to prevent information leaks.

Encrypted Data Processing: Technologies such as homomorphic encryption and trusted execution environments keep data encrypted during processing, reducing the risk of unauthorized access. However, they can be computationally expensive.

Federated and Distributed Analytics: These tools allow analysis of data that remains unseen by analysts. Federated learning, for example, pre-processes data at the source, sending only results to analysts. Reliable connectivity is essential for these tools.

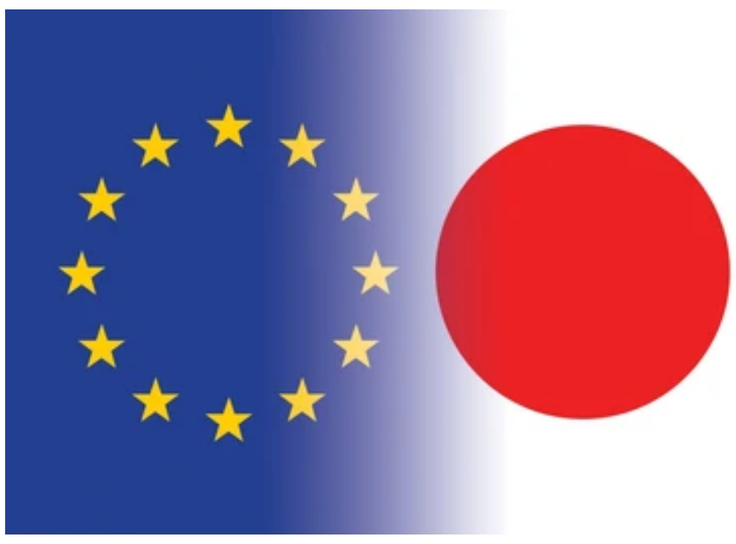
Data Accountability Tools: While not strictly PETs, tools like accountable systems and personal data stores empower individuals to control their data and enforce access rules.

PETs are still developing, with limited use cases and maturity levels. They hold great potential for enhancing privacy and data protection but require careful consideration of their limitations and vulnerabilities.

PRIVACY DIGEST

The European Commission launches Whistleblower Tools for Digital Services Act and Digital Marketing Act

On 29 April 2024, European Commission launched whistleblower tools for the Digital Services Act (DSA) and Digital Markets Act (DMA), allowing individuals to report harmful practices of Very Large Online Platforms (VLOPs) or Search Engines (VLOSEs) under the DSA and violations by gatekeepers under the DMA. These tools enable anonymous reporting in any EU official language and format, with encrypted data and certification by an independent third party to protect whistleblower privacy. Complaints about VLOPs or VLOSEs can be lodged with national Digital Services Coordinators under the DSA, while DMA violations by gatekeepers can be reported to the Commission or national competition authorities.



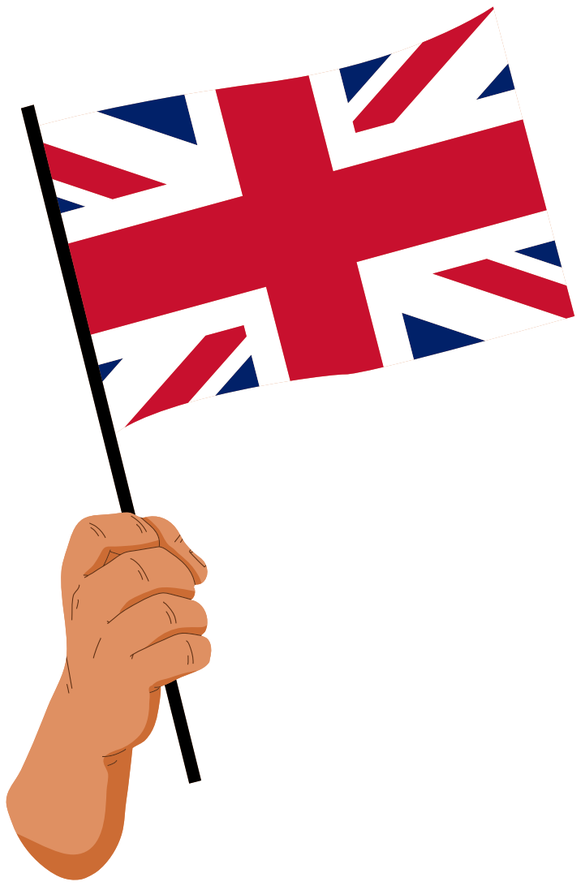
EU-Japan: Council Approves Protocol for Free Data Flow

On 29 April 2024, the Council approved a protocol to enhance the EU-Japan Economic Partnership Agreement. The protocol aims to facilitate cross-border data flows between the EU and Japan by eliminating unjustified data localisation measures. This move will provide legal certainty for businesses, allowing them to handle data more efficiently and without cumbersome administrative requirements. Under the protocol, data localisation requirements will be removed, enabling companies to avoid additional costs associated with maintaining data storage facilities in multiple locations.

MAY 2024 AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

UK implements New Regulations for Cybersecurity in Smart Devices



On 29 April 2024, UK has implemented new regulations mandating minimum-security standards for internet-connected smart devices, making it the first country to introduce such laws. Manufacturers are now required to safeguard consumers from hacking and cyber-attacks by banning weak default passwords and ensuring prompt security updates. The move aims to protect personal privacy, data, and finances, addressing growing concerns over cyber threats as smart devices become increasingly ubiquitous. These measures reinforce the government's commitment to online safety and resilience, contributing to the UK's broader cybersecurity strategy and economic growth objectives.

MEPs Propose Enhanced Customer Control Over Financial Data

On April 18, 2024, MEPs proposed new rules to enhance customer control over financial data. The framework allows customers to grant explicit permission for data usage by financial institutions, fostering innovation and competition. Key provisions include customer consent, liability agreements for data breaches, and exclusion of sensitive data categories. The European Banking Authority will oversee authorization, with small firms granted an extended implementation period for compliance.

PRIVACY DIGEST

‘Large volume’ of data stolen from UN agency after ransomware attack

On April 3, 2024, the United Nations Development Programme (UNDP) disclosed a ransomware attack on its local IT infrastructure in UN City, Copenhagen, resulting in the theft of a substantial amount of internal data, including human resources and procurement information. The breach, attributed to a group named "8Base," potentially exposed sensitive details such as dates of birth, social security numbers, bank account information, and passport details of staff members and contractors. This incident highlights the ongoing cybersecurity challenges faced by UN agencies, with previous breaches reported in recent years.

US passes bill to force TikTok to be sold to US approved company or face nationwide ban

On 23 April 2024, the US House of Representatives overwhelmingly passed a bill aimed at compelling ByteDance, the parent company of TikTok, to divest itself of the app or face a nationwide ban, signaling a landmark move in US social media regulation. Spearheaded by Texas Republican representative Michael McCaul, the legislation underscores bipartisan concerns over Chinese influence and data privacy, despite TikTok's assurances of data independence.

PRIVACY DIGEST

Europe shrugs off Washington’s TikTok fears

Europe remains relatively indifferent to Washington's concerns over TikTok's security risks, contrasting with the U.S.'s move to force the app's sale. While a U.S. bill mandates ByteDance, TikTok's parent company, to sell the app within a year despite fears of Beijing's data access, European leaders have largely refrained from echoing the U.S.'s fervour, attributing their stance to a different perception of national security threats and the effectiveness of existing EU regulations like the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) in safeguarding privacy and online safety.

FTC Finalizes Changes to Health Breach Notification Rule

On 26 April 2024, Federal Trade Commission (FTC) approved changes to the Health Breach Notification Rule (HBNR), enhancing protections for consumers' sensitive health data. The updates clarify the rule's applicability to health apps and similar technologies not covered by HIPAA, expand required content for consumer notices in case of a breach, and authorize broader use of electronic notification methods.

Colorado Passes Landmark Bill Protecting Neural Data Privacy

On 17 April 2024, Colorado Governor Jared Polis signed a groundbreaking bill into law, expanding privacy protections to include biological and neural data. The legislation, passing with resounding bipartisan support, aims to safeguard intimate information collected by consumer neurotechnologies. Advocates hail it as a critical step in defending individuals' privacy rights amid the rapid advancement of brain-monitoring technologies.

PRIVACY DIGEST

European Parliament Advances Data Protection Enforcement Measures

On April 10, 2024, the European Parliament advanced measures to strengthen data protection enforcement. MEPs agreed on standardized deadlines, improved access to information, and clarity on amicable settlements under the GDPR. Rapporteur Sergey Lagodinsky emphasized the fundamental right to data protection. The file now moves to inter-institutional negotiations, with further action expected after the European elections in June.

Canada's Privacy Commissioner Joins Global Cooperation Arrangement

9 April 2024: The Office of the Privacy Commissioner of Canada (OPC) has officially become a member of the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE). This move is a prerequisite for Canada's participation in the Global Cross-Border Privacy Rules Forum (Global CBPR), to which it committed in April 2022, joining several other nations. Earlier ICO had also joined on 4 April 2024. This agreement allows the ICO to collaborate with member countries, including the United States, Australia, Canada, Mexico, Japan, the Republic of Korea, the Philippines, Singapore, and Chinese Taipei, without needing separate agreements.

PRIVACY DIGEST

Personal Information Protection Commission

Personal Information Commission Releases Guide for Overseas Businesses on Korean Data Protection Laws

On April 8 2024, the Personal Information Commission released the "Guide to Application of Personal Information Protection Act for Overseas Businesses," offering case-based guidance on compliance with the Personal Information Protection Act. It emphasizes equal treatment between domestic and foreign businesses and outlines legal obligations, including reporting data leaks and designating a domestic agent. The guide aims to ensure clarity and compliance with Korean data protection laws.

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.