PRIVACY ROUND UP

AZURE DATA PROTECTION CONSULTANTS LLP

2023

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

PRIVACY ROUND UP

India

Enactment of Digital Personal Data Protection Act (DPDPA)

India enacted the Digital Personal Data Protection Act (DPDPA) fortifying its data protection framework and emphasizing the commitment to safeguarding citizens' personal data. It was announced that the anticipated draft rules for the DPDPA are nearing completion, expected to be released soon for public consultation. Additionally, Sanket S. Bhondve, an IAS officer, was appointed to lead the formation of the DPB, responsible for overseeing DPDPA implementation and ensuring data fiduciary compliance.

IRDAI Formed A Task Force To Assess DPDP Act's Impact

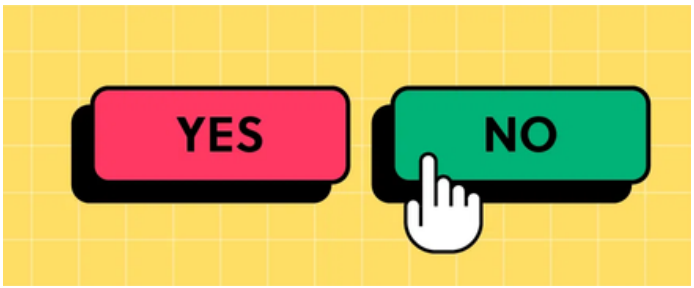
IRDAI formed a task force to evaluate the impact of the Digital Personal Data Protection Act, 2023, on the insurance sector. The task force, comprising industry leaders, aims to submit a comprehensive report within one month.

MEITY Issued Rules for Online Gaming Companies

MEITY issued Online Gaming Rules amending the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Under these rules, online gaming companies face due diligence requirements, and KYC procedures, emphasizing responsible gaming practices.

PRIVACY ROUND UP

India



Guidelines on Dark Patterns Released

The Department of Consumer Affairs in India released proposed guidelines to curb deceptive marketing tactics, often referred to as "dark patterns." These guidelines emphasize the need to regulate marketing strategies that involve forced actions, false urgency, and disguised advertisements. The aim is to protect consumers from negative targeting by companies employing such tactics.

Saudi Arabia

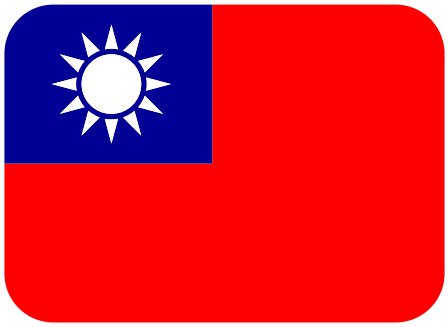
Personal Data Protection Law (PDPL) Came into Effect

The Personal Data Protection Law (PDPL) is a comprehensive national data protection law regulating personal data processing and collection in Saudi Arabia. Enacted in September 2023, this law is applicable to businesses operating within Saudi Arabia or those handling the personal data of Saudi residents. Notably, these entities are granted a grace period of one year to align their practices with the new regulations, as enforcement is set to commence on September 14, 2024.

PRIVACY ROUND UP

Taiwan

Amendments to Personal Data Protection Act Implemented



The Legislative Yuan in Taiwan implemented amendments to the Personal Data Protection Act (PDPA) to bolster data protection standards and regulatory oversight in the country. Key updates include imposing substantial financial penalties, ranging from NTD20,000 to NTD2 million, for violations of data security provisions. Additionally, non-compliance penalties, ranging from NTD150,000 to NTD15 million, have been introduced to ensure prompt corrective actions in case of data security incidents. Furthermore, the amendments extend data protection obligations to non-government agencies, compelling them to adhere to PDPA provisions. A regulatory authority has also been established to oversee compliance across various entities.

Vietnam

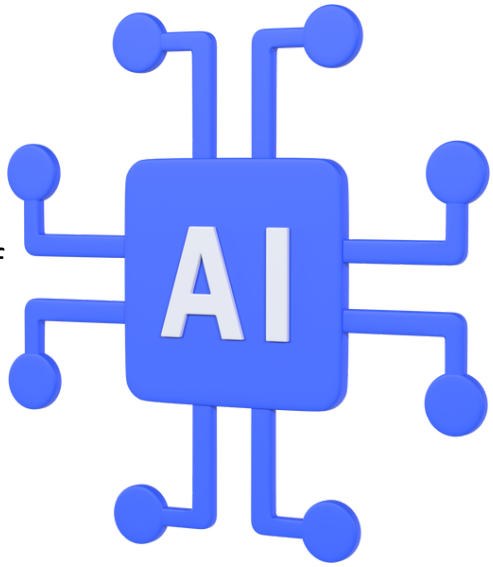
The Protection of Personal Data Decree Was Implemented

Vietnam's much-anticipated comprehensive privacy law, the Protection of Personal Data Decree, came into effect on July 1, 2023, marking a significant milestone in the country's data protection framework. This new law includes key provisions that address data subject rights, cross-border transfer of personal data, and requirements for data controllers, processors, and third parties. Additionally, the law specifies rules on privacy notices, processing of children's personal data, and measures to protect sensitive personal data.

PRIVACY ROUND UP

Canada

Voluntary Code of Conduct and Principles for Generative AI Released



Canada unveiled a voluntary code of conduct for generative artificial intelligence (AI) to guide entities in the development and use of AI systems, emphasizing safety, fairness, transparency, and human oversight. Additionally, the Office of the Privacy Commissioner of Canada has released principles focusing on the trustworthy development and deployment of generative AI, stressing compliance with data protection laws, obtaining legal authority and consent for using personal information, and aligning data collection with a specific purpose.

Ongoing Developments in Canadian Legislation

Canada advanced Bill C-27, also known as the Digital Charter Implementation Act, that proposes amendments to the Personal Information Protection and Electronic Documents Act and introduces three new laws. These include the Artificial Intelligence and Data Act, the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act. As part of the developments, Minister François-Philippe Champagne submitted amendments to the Standing Committee on Industry and Technology, but there's skepticism about the bill passing in its current form before the potential federal election in 2025.

PRIVACY ROUND UP

Canada

Guide for Mitigating Generative AI's Cybersecurity Risks Issued

The Canadian government issued cybersecurity guidance on the use of generative artificial intelligence (AI). This comprehensive document defines generative AI, highlights its applications, outlines associated risks, and provides effective risk mitigation recommendations for organizations and individuals.

TikTok Banned on Government-Issued Devices

In response to security concerns, the Canadian government, led by Treasury Board President Mona Fortier, has prohibited TikTok on government-issued devices. This decision is based on the assessment that TikTok poses an unacceptable risk to privacy and security. The government reaffirms its commitment to regularly monitoring systems and taking necessary actions to address risks, prioritizing the security of government information.

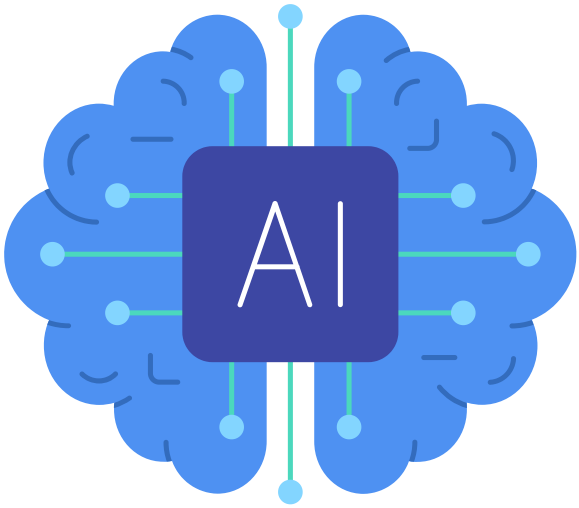
Office of the Privacy Commissioner's 2023-2024 Departmental Plan Released

The Office of the Privacy Commissioner of Canada unveiled its 2023-2024 departmental plan. Commissioner Philippe Dufresne acknowledges the office's readiness to deliver on its new mandate pending federal privacy law reforms under Bill C-27. The plan underscores the need for resources to accommodate operational and structural changes, prioritizing the establishment of a fair, accessible, and timely compliance process.

PRIVACY ROUND UP

U.S.A.

Executive Order Issued to Ensure Responsible AI Development



President Biden issued an executive order to promote the responsible development and use of AI. The order paves the way for new standards on AI safety, security, privacy, equity, civil rights, consumer protection, worker support, innovation, competition, and American leadership worldwide. It includes provisions to protect privacy, such as prioritizing federal support for privacy-preserving AI techniques.

‘My Health, My Data' Act! Was Signed into Law

The 'My Health, My Data' Act empowers Washington State residents to manage their health information. This law grants individuals the right to access, control, and delete their health data, including the ability to request a complete list of entities with whom their data has been shared. The law's extraterritorial scope extends to companies that process health data of Washington State residents, regardless of their location.

California Enacted the Delete Act

California enacted the Delete Act, granting residents the authority to demand the removal of their personal information from data brokers. This law formally categorizes data brokers as entities that collect, assemble, and sell personal information of California residents. The act mandates the creation of a centralized portal for Californians to easily submit deletion requests.

PRIVACY ROUND UP

U.S.A.

California Privacy Rights Act Entered Into Effect

Building upon the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), effective from January 1, 2023, strengthens privacy protections for California residents by expanding its scope and enhancing employee control over personal data. It also mandates clear opt-out options for sensitive information sharing and requires privacy risk assessments and annual cybersecurity audits for specific organizations.

New York Enacted a Law Prohibiting Distribution of Explicit Deepfakes

Governor Kathy Hochul, a Democrat from New York, signed a bill into law that prohibits the distribution of AI-generated deepfake content portraying non-consensual sexual images. Violating this law could result in a one-year jail sentence. Additionally, victims have the option to pursue a private right of action in civil court for damages.

Connecticut Governor Signed Bill on AI

Connecticut Governor Ned Lamont signed SB 1103, legislation focused on artificial intelligence, automated decision-making, and personal data protection. This act, SB 1103, introduces several key provisions. It establishes an Office of Artificial Intelligence, which will serve as a dedicated entity for overseeing AI-related matters well as a task force to study AI and develop an AI bill of rights.

PRIVACY ROUND UP

State Landscape

The following regulations were signed into law this year:

- Tennessee Information Protection Act - TIPA is scheduled to be enforced starting July 1, 2024.
- Delaware Personal Data Privacy Act - DPDPA will take effect on January 1, 2025.
- Indiana Consumer Data Protection Act - This legislation is set to take effect on January 1, 2026.
- Iowa Consumer Data Protection Act - This act is scheduled to be enforced starting January 1, 2025.
- Montana Consumer Data Privacy Act - Its implementation is slated for October 1, 2024.
- Oregon Consumer Privacy Act - This legislation is set to become effective on July 1, 2024.
- Florida's Digital Bill of Rights - The law will take effect July 1, 2024.
- Texas Data Privacy And Security Act - The TDPSA is scheduled to take effect on July 1, 2024

This year, the following regulations became effective:

- Colorado Privacy Act - The Colorado Privacy Act, signed into law on July 8, 2021, mirrors the Virginia Consumer Data Protection Act (VCDPA). Operationalized through CPA Rules, the associated regulations became effective on July 1, 2023.
- Connecticut Data Privacy Act - Governor Ned Lamont, a Democrat from Connecticut, endorsed Senate Bill 6, titled 'An Act Concerning Personal Data Privacy and Online Monitoring' (CTDPA), into law on May 10, 2022. The legislation officially came into effect on July 1, 2023.
- Utah Consumer Privacy Act - Utah Governor Spencer J. Cox signed the Utah Consumer Privacy Act (UCPA) into law on March 24, 2022. The legislation is scheduled to be enforced starting from December 31, 2023.
- Virginia Consumer Data Protection Act - The Virginia Consumer Data Protection Act was enacted into law in 2021 and became officially effective on January 1, 2023.

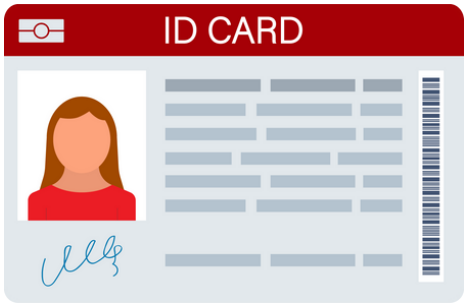
PRIVACY ROUND UP

Philippines

NPC Released Guidelines On Consent

The National Privacy Commission (NPC) published, following its public consultation, the NPC Circular No. 2023-04 Guidelines on Consent. In particular, the Circular applies to personal information controllers (PICs) engaging in the processing of personal data based on the consent of the data subject.

NPC Issued Guidelines On Identification Cards



The National Privacy Commission (NPC) published NPC Circular No. 2023 – 03 Guidelines on Identification Cards that apply to private organizations that issue identification cards to data subjects, encompassing both physical and digital formats. The guidelines cover a range of identification cards, including but not limited to company IDs, school IDs, insurance cards, membership cards, and rewards or loyalty cards. The guidelines mandate ID cards to capture only essential personal data, with additional information allowed if required by law. Issuing organizations must implement safeguards following technological standards, bearing the responsibility to demonstrate the proportionality of data inclusion. Violations incur criminal, civil, and administrative liabilities under the country's data privacy law.

NPC Sought Input on Draft Guidelines on Legitimate Interest

The National Privacy Commission (NPC) launched a public consultation on the draft circular on guidelines on legitimate interest. Through this draft circular, the NPC aims to provide guidelines for personal information controllers and third parties relying on legitimate interest as a lawful basis to process personal information.

PRIVACY ROUND UP

UK

The Data Protection and Digital Information Bill Moved Forward

The Data Protection and Digital Information Bill has advanced as it passed the report stage and received a third reading in the House of Commons on November 29, 2023. The bill then proceeded to the House of Lords for further consideration. The first reading in the House of Lords occurred on December 6, marking the beginning of the bill's progress through the Lords.

UK-US Data Bridge Became Effective

The UK-US Data Bridge, effective from October 12, 2023, is a mechanism allowing the transfer of personal data from the UK to the US without additional safeguards. Implementation of the Data Bridge involves requirements for both UK and US organizations, including the updating of privacy policies and certification to the Data Privacy Framework List.

UK Parliament Approved Online Safety Bill with Stringent Penalties

The U.K. Online Safety Act received royal assent on 26 October, establishing new obligations for how technology companies were to "design, operate, and moderate their platforms."

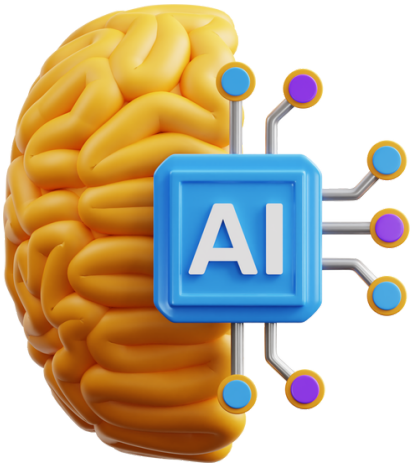
PRIVACY ROUND UP

G20

Leaders Reaffirmed Commitment to AI Collaboration and Privacy

During their meeting in New Delhi, India, G20 leaders reaffirmed their commitment to collaboration on artificial intelligence and privacy matters. These topics were highlighted within the context of the leaders' dedication to technological transformation and the development of digital public infrastructure. The declaration included a dedicated section emphasizing the responsible use of AI for the benefit of all, as well as the significance of ensuring the secure and lawful flow of data across borders while fostering trust.

G7



Leaders Adopted International Guidelines and Code of Conduct for AI Systems

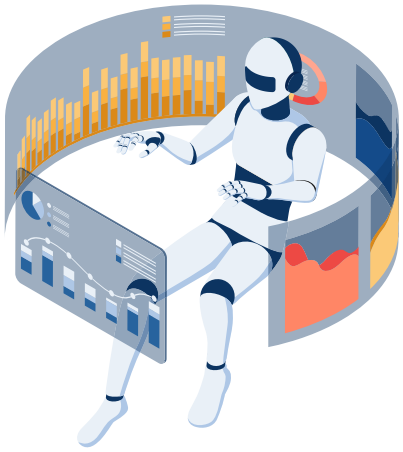
On October 30, 2023, G7 leaders announced their endorsement of both the International Guiding Principles on Artificial Intelligence and an International Code of Conduct for Advanced AI Systems. These evolving principles are designed to navigate the dynamic landscape of advanced AI, emphasizing the cultivation of benefits and mitigation of risks. Applicable to all AI actors, the principles cover the spectrum of advanced AI systems, addressing aspects from design and development to deployment and use. The accompanying Code of Conduct provides further elaboration on these guiding principles, collectively forming a comprehensive framework for responsible AI practices on the international stage.

PRIVACY ROUND UP

South Korea

Amendment to Personal Information Protection Act Approved

The State Council of the Republic of Korea granted approval for an amendment to the Enforcement Decree of the Personal Information Protection Act (PIPA). The newly approved enforcement regulations officially took effect on September 15th. The primary focus of this amendment is the harmonization of standards for processing personal information across various sectors.



PIPC Introduced AI Privacy Unit in South Korea

The Personal Information Protection Commission (PIPC) in South Korea established an Artificial Intelligence Privacy Team. This team is dedicated to formulating principles specifically applicable to artificial intelligence contexts, moving beyond the confines of existing regulations. The PIPC's objective is to develop a "principle-centred" disciplinary framework, addressing uncertainties that companies may encounter in the realm of AI.

PIPC Published Guidelines for AI and Personal Data in South Korea

South Korea's Personal Information Protection Commission issued guidelines for the utilization of personal data in support of artificial intelligence technologies. These guidelines outline principles for processing personal information at various stages of AI development, offering timely legal interpretation and consulting support. The PIPC emphasizes that these guidelines not only align with current regulations but also serve as a blueprint for jointly designing a regulatory system in the future for both the government and the private sector.

PRIVACY ROUND UP

EU

EU Lawmakers Reached Landmark Agreement on AI Act

As a result of three days of marathon talks between the Council presidency and the European Parliament's negotiators, the European Parliament reached a provisional agreement on the first-ever global rules for artificial intelligence (AI). This is a major step forward for ensuring that AI systems used in Europe are safe, fair, transparent, and respect fundamental rights.

European Parliament Passed the Data Act

The European Parliament approved the Data Act, that aims to promote an equitable and innovative data economy in the European Union. This legislation addresses challenges in data access, control, and value creation. Key provisions include enhancing data portability, promoting fair data sharing, empowering small and medium-sized enterprises, and facilitating cloud switching. These measures collectively aim to empower individuals and businesses, encourage fair practices, and foster a dynamic and competitive data-driven ecosystem in the EU.

EU Data Governance Act Became Effective

The EU Data Governance Act officially toke effect for covered entities as of September 24. Enacted in June 2022, this legislation aims to enhance access to public-sector data for the development of new products and services. Covered entities were provided a 15-month grace period to ensure compliance with the new regulations.

PRIVACY ROUND UP

EU

EDPB Issued Urgent Binding Decision Banning Meta's Behavioral Advertising Across EEA

The European Data Protection Board released the text of its urgent binding decision, directing Ireland's Data Protection Commission (DPC) to implement a European Economic Area-wide ban on Meta's personal data processing for behavioural advertising. This decision comes in response to a request from Norway's data protection authority, Datatilsynet, seeking a final order on the issue from the EDPB. The DPC had previously issued a decision on November 10th.

EC Introduced Data Privacy Framework for Personal Data Transfers from EEA to US

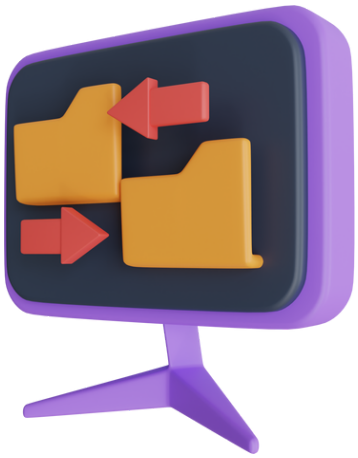
The European Commission issued an adequacy decision affirming that the United States provides a level of data protection equivalent to EU standards. This decision enables secure data transfer from the EU to U.S. companies within the Data Privacy Framework without the need for additional safeguards. The 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.

PRIVACY ROUND UP

China

Interim Measures for the Management of Generative AI Services Became Effective

China introduced the 'Interim Measures for the Management of Generative Artificial Intelligence Services,' effective from August 15, enforced by the Cyberspace Administration of China (CAC). These regulations apply to generative AI services accessible to the public, including those provided by offshore companies for Chinese residents. The rules require alignment with socialist core values and emphasize non-discrimination in algorithm design, respect for intellectual property and business ethics, protection of privacy and personal information, transparency in AI services, and the implementation of security assessments to prevent illicit activities. Offshore providers must also comply with these regulations.

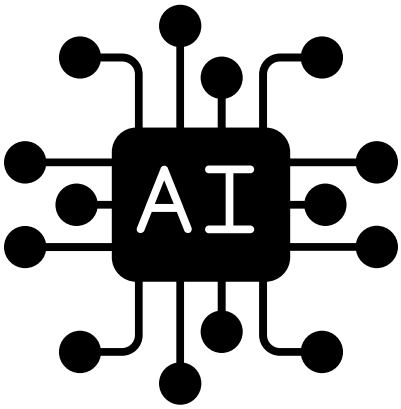


Standard Contract Clauses for Cross-border Data Transfer Were Announced

The Cyberspace Administration of China (CAC) announced the final versions of the "Measures for the Standard Contract for Cross-border Transfer of Personal Information" and the "Standard Contractual Clauses for Cross-border Transfer of Personal Information" on February 22, 2023, in line with the Personal Information Protection Law. These measures came into effect on June 1, 2023.

Global AI Governance Initiative Introduced

The Cyberspace Administration of China introduced its "Global AI Governance Initiative," outlining a framework for the regulation of artificial intelligence. The framework emphasizes the need for "equal rights" in AI development, irrespective of a country's size, strength, or social system.



PRIVACY ROUND UP

Singapore

Public Consultation Launched for Guidelines on the Use of Personal Data in AI

The Personal Data Protection Commission of Singapore initiated a public consultation on the 'Proposed Advisory Guidelines On Use Of Personal Data In AI Recommendation And Decision Systems.' This guidance aimed to gather feedback on the appropriate utilization of personal data in AI systems, in accordance with The Personal Data Protection Act 2012.

Cybersecurity Guidelines for the Healthcare Sector Released

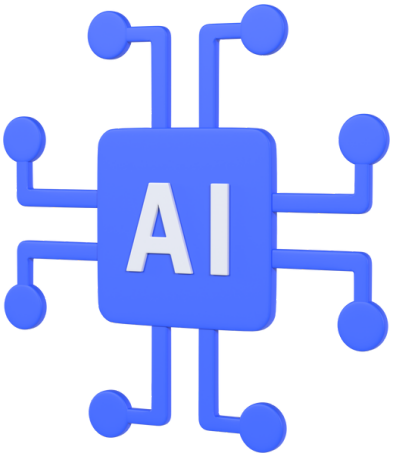
Singapore's Ministry of Health and the Cybersecurity Agency of Singapore released cybersecurity guidelines for healthcare providers. These guidelines emphasize the critical importance of securing data, keeping software updated, and having a well-planned response in the event of a data breach. Additionally, the Ministry of Health is planning to introduce the Health Information Bill in 2024, which is aimed at governing the safe and secure collection, access, use, and sharing of health information.

PRIVACY ROUND UP

Indonesia

Draft Regulation of Personal Data Protection Law Released

Indonesia released its draft regulation ("Draft Regulation") for the implementation of the Personal Data Protection Law (PDPL) in August 2023. The nation sought public input, encouraging comments and suggestions from citizens, businesses, and experts. The consultation period concluded on September 14th, providing a valuable opportunity for stakeholders to contribute insights. The implementation is expected to take place in October 2024.



Guidelines for AI Ethics Released

The Indonesian government has taken a step toward responsible AI development by drafting ethics guidance for developers using artificial intelligence (AI). According to a ministerial draft this move aims to prevent potential misuse of the technology.

Nigeria

Nigeria's President Approved Data Protection Bill

President Bola Tinubu signed the Nigeria Data Protection Bill, 2023 into law on June 12th. The new law establishes the Nigeria Data Protection Commission, which will be led by a national commissioner responsible for overseeing the processing of personal information by entities. Among its responsibilities, the NDPC is tasked with promoting the development of personal data protection technologies in line with international best practices.

PRIVACY ROUND UP

Data Breaches

MOVEit

The widespread breach of the file transfer tool MOVEit affected numerous organizations, exposing the personal information of millions. The attack began with a security vulnerability in MOVEit's software. Although MOVEit addressed the flaw after discovering it, hackers had already accessed a significant amount of sensitive data. The Clop ransomware group, linked to Russia, has claimed responsibility for the breaches and issued threats to publish the stolen information on the dark web.

23andMe

In October, it was reported that a data breach occurred at the genetic testing firm 23andMe, affecting 6.9 million individuals—a substantial increase from the initial estimate of about 14,000 people. The broader impact of the breach was revealed when the company identified that individuals utilizing the consent-based DNA Relatives feature, which automatically shares some of their data with others, had their information compromised by hackers. Stolen genetic data from users of the service may include first and last names, email addresses, birth dates, and information stored by 23andMe regarding users' genetic ancestry and history.

T-Mobile

In May, T-Mobile disclosed its second data breach of 2023, wherein over 800 customers' PINs, full names, and phone numbers were exposed. The initial breach occurred in early January 2023 when T-Mobile found that a malicious actor had infiltrated their systems in November of the previous year, compromising personal information such as names, emails, and birthdays for more than 37 million customers. T-Mobile not only incurred significant financial losses due to security vulnerabilities but also eroded customer trust with multiple breaches exposing personal information.

PRIVACY ROUND UP

Data Breaches

Yum! Brands (KFC, Taco Bell, & Pizza Hut)

In April 2023, Yum! Brands, the parent company overseeing well-known fast-food chains like KFC, Taco Bell, and Pizza Hut, reported a cyber attack that took place in January. Initially, they thought the attack had solely impacted corporate data, but later they informed employees who might have had their personal information compromised.

ChatGPT

In late March, ChatGPT encountered a setback with the revelation of a data breach. A software glitch led to the inadvertent exposure of payment-related details for 1.2% of ChatGPT Plus subscribers who were active during a specific nine-hour period. Additionally, certain users may have had the ability to view the complete names, email addresses, payment details, and credit card information of other active users.

Activision

Activision, the video game publisher of Call of Duty, confirmed a data breach on February 19th. The breach involved an SMS phishing attack on an HR employee, granting unauthorized access to employee data, including emails, phone numbers, salaries, and work locations. Activision addressed the breach promptly, asserting that insufficient data was obtained to warrant immediate employee alerts. However, a security research group revealed that the hacker also accessed the company's 2023 release schedule along with sensitive employee information.

PRIVACY ROUND UP

Data Breaches

Google Fi

Google Fi disclosed a data breach involving a third-party system that stored a "limited amount" of customer data. The stolen data comprised account activation dates, details about specific mobile plans, and SIM card serial numbers. Authorities maintain that no personally identifiable information was taken from customers. However, the name of the third-party service provider affected by the data breach was not revealed.

Indian Council of Medical Research

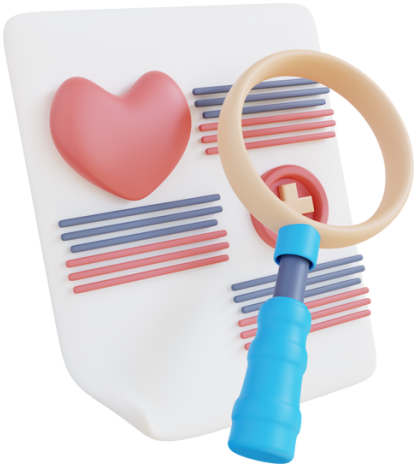
In October, the personal data of 815 million Indian residents, reportedly taken from the ICMR's Covid-testing database, was found being sold on the dark web. Resecurity, a security company that identified the listing, reported that the data encompassed individuals' names, ages, genders, addresses, passport numbers, and Aadhaar numbers (a 12-digit government identification number).

Air Canada

In September, Air Canada revealed that it had encountered a cyberattack, leading to the compromise of personal data belonging to its employees. Peter Fitzpatrick, a spokesperson for Air Canada, clarified that the hackers did not breach the airline's customer-facing systems or flight systems. However, specific information regarding the types of personnel records accessed and the exact number of affected employees was not disclosed.

PRIVACY ROUND UP

Data Breaches



Hamilton Health Services

In 2023, Hamilton Health Services reported a total of 11 privacy breaches to the Information and Privacy Commission of Ontario. One of these instances involves eight former employees accessing the personal health information of 4,000 patients. The Information and Privacy Commission of Ontario has launched an investigation and is evaluating any potential systemic issues contributing to such incidents.

Toyota

In May, Toyota acknowledged that the exposure of vehicle data from more than 2 million Japanese customers was a result of "human error." The company admitted that identification numbers and location data of vehicles registered on Toyota's main cloud service platform since 2012 were unintentionally made publicly accessible. The data remained exposed for a decade due to the cloud system being mistakenly set to public instead of private.

Ring

Amazon’s smart doorbell company Ring’s data was stolen by the ransomware gang ALPHV. Ring has not found any evidence of a direct breach but said that a third-party vendor was attacked by ransomware. However various sources have verified that the stolen data was posted on the group’s data forum.

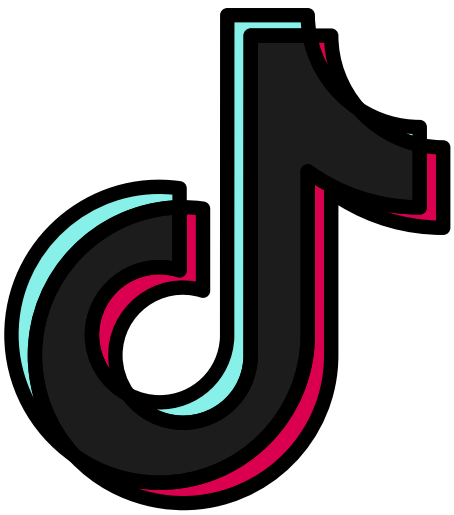
PRIVACY ROUND UP

Fines And Penalties

Meta Faced Unprecedented Penalties for GDPR Violations and Unauthorized Data Transfers

In May, Meta Platforms Ireland, the parent company of Facebook, faced a historic fine of 1.2 billion euros imposed by Ireland's Data Protection Commission under the European Union's General Data Protection Regulation. The substantial penalty was attributed to alleged unauthorized data transfers from the EU to the U.S. Additionally, in January, the Irish DPC levied a combined fine of €390 million against Meta, citing breaches of the GDPR. Notably, after consultation with the European Data Protection Board (EDPB), it was determined that Meta can no longer rely on the GDPR's "performance of a contract" legal basis for processing personal data in the context of behavioral advertising.

TikTok Faced Substantial Fines and Regulatory Scrutiny by Irish DPC and ICO

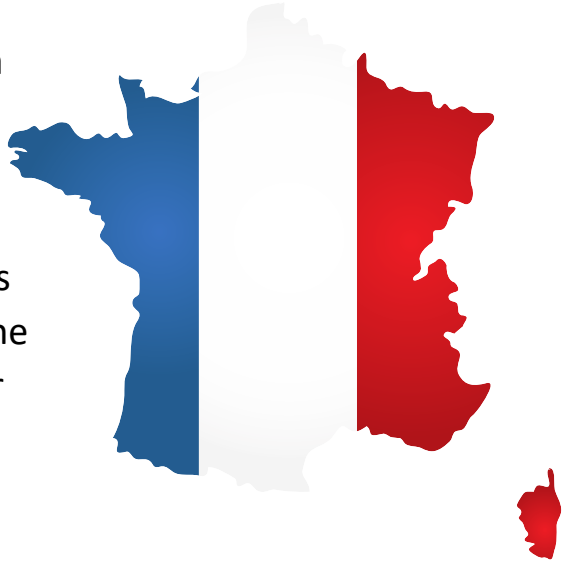


TikTok faced significant regulatory action on multiple fronts. The Irish Data Protection Commissioner (DPC) has fined the platform €345 million for breaching GDPR rules, including exposing 13-17-year-old users by default to a public setting and inadequately verifying adults in the 'family pairing' scheme. Concurrently, the UK's Information Commissioner's Office (ICO) imposed a £12.7 million fine on TikTok for illegal data processing of 1.4 million children under 13. The ICO identified TikTok's failure to prevent underage access and deficiencies in ensuring lawful data processing. In response, the ICO introduced a Children's Code to enhance digital protections for children.

PRIVACY ROUND UP

Fines And Penalties

Criteo Hit with €40 Million Fine by French Data Protection Authority



The French Data Protection Authority (CNIL) has imposed a €40 million fine on Criteo, an online advertising specialist, following complaints lodged by non-profit organizations Privacy International and None of Your Business (NOYB). CNIL's decision is based on Criteo's failure to ensure that its partners, including publishers, obtained user consent for the use of Criteo's cookies. While the primary responsibility for obtaining consent lies with the partners, CNIL holds Criteo accountable for verifying this consent. The €40 million penalty represents approximately 2% of the company's global revenue, reduced from CNIL's initial proposal of €60 million by rapporteurs.

WhatsApp Fined €5.5 Million by Irish DPC

An amount of €5.5 million has been levied against WhatsApp Ireland Ltd by the Irish watchdog for compelling users to consent to the utilization of their personal data for "service improvements and security." This case mirrors the one involving Meta Platforms Ireland Ltd, originating from May 2018. Alongside the fine, WhatsApp Ireland Ltd has received an order to align its data processing operations with EU privacy regulations within a six-month period.

PRIVACY ROUND UP

Fines And Penalties

Spotify Hit with €4.9 Million Fine in Sweden for Breaching User Data Access Rights

The music streaming platform Spotify faced a fine of SEK 58 million (€4.9 million) in Sweden for violating the data access rights of its users. The Swedish Authority for Privacy Protection (IMY) discovered that Spotify lacked transparency in how it collected and utilized user data. Given Spotify's international usage, the ruling was coordinated with other data protection authorities in the EU.

Clearview AI Faced Additional €5.2 Million Penalty for Non-Compliance with French Data Protection Directives

Clearview AI Inc. found itself in trouble once more as it failed to adhere to the directives of the French regulator. Despite being fined €20 million and instructed not to collect and process the data of individuals in France without a legal basis, Clearview AI did not cooperate within the two-month stipulated period. Consequently, the French regulator, CNIL, imposed a penalty payment of €5.2 million, to be paid in addition to the outstanding fine.

Azure Data Protection Consultants LLP

Contact us for any queries:

http://www.azuredpc.com

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com