Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

October 2024

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

OCTOBER 2024 — AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

October is Cybersecurity Awareness Month!

Welcome to our October newsletter! As the leaves change and the air gets cooler, we're focusing on an important topic: cybersecurity. This month, we celebrate Cybersecurity Awareness Month, a time to highlight the need for online safety and to share knowledge that can help protect your digital life.

With online threats becoming more common, it's essential to know what to watch out for. In this edition, we'll explore everyday online risks and share simple tips to enhance your security. Simple habits like being cautious with emails and links can go a long way in keeping you safe.

We'll also share resources to help you stay informed about the latest trends and threats in cybersecurity. Remember, keeping safe online is something we can all do together, so we encourage you to talk about safe online practices with friends and family.

Let's make the most of Cybersecurity Awareness Month by prioritizing our online safety and working together to create a secure digital environment. Thank you for being part of our community!

PRIVACY DIGEST

ASIA PRIVACY UPDATES

TRAI Releases Recommendations on Service Authorizations Under Telecommunications Act

On September 18, 2024, the Telecom Regulatory Authority of India (TRAI) recommended a new framework for service authorizations under the Telecommunications Act. Key proposals include the government issuing concise authorizations instead of formal agreements. TRAI emphasized privacy and data protection, requiring authorized entities to safeguard communication privacy and prevent unauthorized interception. It also recommended that network infrastructure and data storage must be located in India, with monitored encryption use and strict rules for third-party data privacy.

DSCI Issues Privacy Guidelines for Healthcare Sector

The Data Security Council of India (DSCI) has issued privacy guidelines for the healthcare sector, focusing on protecting patient data amid increasing digitalization. The guidelines emphasize accurate data collection, informed consent, secure data handling, patient access to data, and maintaining anonymity where possible. They aim to help healthcare providers, pharmacies, and insurers handle sensitive health information responsibly, ensuring patient privacy and data security.

DSCI Publishes Whitepaper on Cross-Border Data Transfers

On September 17, 2024, the DSCI released a whitepaper providing guidance on managing cross-border data transfers for Indian organizations. It outlines legal responsibilities under the Digital Personal Data Protection Act and offers best practices, including conducting risk assessments, implementing audit mechanisms, and enhancing protections for sensitive data. The whitepaper also recommends following sector-specific regulations and adhering to industry standards like ISO 27701:2019.

PRIVACY DIGEST

Privacy Watchdog Cautions Hong Kong Jobseekers on 'Blind' Ads

Hong Kong's Privacy Commissioner, Ada Chung, warns jobseekers to be cautious of “blind” job advertisements that don't reveal the employer's identity. This follows investigations into five firms for illegal data collection practices. Jobseekers are urged to verify employers before sharing personal information, as these ads could be linked to scams. The Privacy Ordinance requires lawful data collection, and recruitment agencies must protect candidate confidentiality.

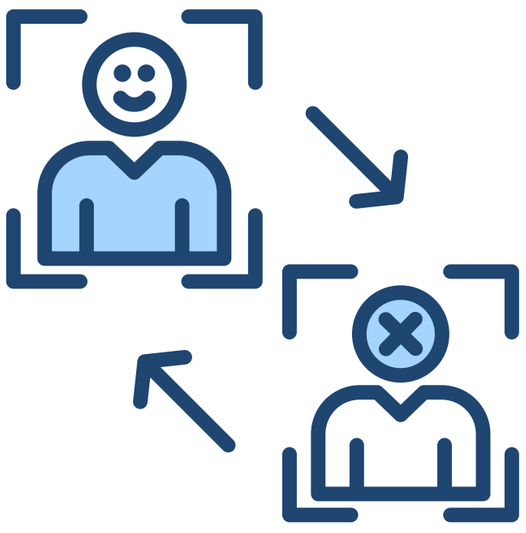
Hong Kong's Privacy Commissioner Investigates LinkedIn's Privacy Policy

The Office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong has launched an investigation into LinkedIn Corporation's updated privacy policy, which allows the use of users' personal data and content to train generative AI models. The PCPD raised concerns about LinkedIn's default opt-in setting, questioning whether it genuinely reflects users' consent. LinkedIn users are encouraged to review the policy changes and modify their settings if they wish to prevent their data from being used for AI training.

Hong Kong Updates GBA Personal Information Filing Guidelines

On October 7, 2024, Hong Kong's Digital Policy Office revised the filing guidelines for the Standard Contract for Cross-boundary Flow of Personal Information in the Greater Bay Area. Hong Kong contracting parties must now submit a completed filing form and proof of identity within 10 working days of signing the contract. The office will check submissions for completeness and may request further documentation. Any changes to cross-boundary transfers will require a new impact assessment or contract, along with updated filing procedures.

PRIVACY DIGEST



Singapore Passes Bill to Ban Deepfake Election Ads

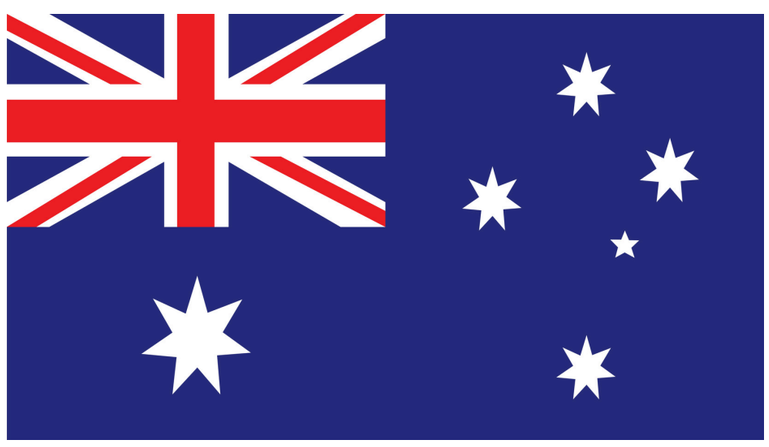
On October 15, 2024, Singapore's Parliament passed Bill No. 29/2024, the Elections (Integrity of Online Advertising) (Amendment) Act 2024. This law prohibits manipulated online election advertising that features deepfakes of candidates. It criminalizes the publication of online election ads containing realistic yet false audiovisual representations made using digital means, such as generative AI, during election periods. The bill specifically targets ads that misrepresent candidates by making them appear to say or do things they did not, with the intent to deceive the public.

Singapore Launches Updated Safe App Standard 2.0

On October 15, 2024, the Cyber Security Agency of Singapore (CSA) unveiled the Safe App Standard 2.0 (SAS), aimed at enhancing security controls for high-risk mobile app developers and providers. This updated standard, which builds on the original released in January 2024, seeks to combat mobile malware and scams, particularly for apps managing sensitive transactions and data. While non-binding, the SAS outlines eight key security areas, such as authentication and cryptography, and introduces four additional cybersecurity areas. It also integrates elements from the ENISA Smartphone Secure Development Guidelines and the MAS Risk Management Guidelines.

Australia's Cyber Security Bill 2024 Introduced

On October 2, 2024, the Australian Government introduced the Cyber Security Bill 2024, aimed at enhancing national cyber security. Key features include mandatory security standards for internet-connected products, reporting obligations for ransomware payments, and the establishment of a Cyber Incident Review Board. The bill also seeks to clarify obligations under the Security of Critical Infrastructure Act 2018 and improve information sharing and risk management practices.



PRIVACY DIGEST

Indonesia Completes UNESCO AI Readiness Assessment

On October 8, 2024, Indonesia, via Kominfo, became the first Southeast Asian nation to complete UNESCO's AI Readiness Assessment. The assessment offers a roadmap for AI policy development, highlighting AI's social and economic impacts while identifying gaps that may lead to bias. Key recommendations include establishing ethical AI governance, creating a National Artificial Intelligence Agency, and emphasizing capacity building and inclusive AI engagement with researchers and startups.

EU PRIVACY UPDATES

NIS2 Cyber Law Takes Effect from 18 October

The new EU cyber law, NIS2, expands cybersecurity rules to more sectors and requires stricter measures for risk management, incident reporting, and senior management accountability. Organizations in key sectors like managed services, food distribution, and chemicals must comply, while others should assess the impact on their critical service providers. Now is the time to review and update your cybersecurity practices.

ESAs Respond to Commission's Rejection of DORA Draft

On 15 October 2024, the European Supervisory Authorities (ESAs) addressed the European Commission's rejection of their draft under the Digital Operational Resilience Act (DORA). The Commission opposed mandatory use of Legal Entity Identifiers (LEI) for ICT service providers, proposing an option for the European Unique Identifier (EUID). The ESAs defended the LEI for global consistency but suggested a dual-identifier system with LEI prioritized. Minor technical changes to the draft were also proposed.

PRIVACY DIGEST

CJEU Rules on DPA Corrective Powers in Data Breach Cases

On 26 September 2024, the Court of Justice of the European Union (CJEU) ruled in Case C-768/21 regarding the corrective powers of data protection authorities (DPAs) in personal data breach cases under the GDPR. The Court determined that DPAs are not required to impose fines or corrective actions if the data controller has proactively implemented necessary measures to address the breach.

European Credit Sector Associations Call for Stronger Fraud Prevention

On 17 September 2024, the European Credit Sector Associations, including EACB, EBF, and ESBG, endorsed the Euro Retail Payments Board's report on retail payment fraud. The report identifies four key actions for improving fraud prevention: enhancing cross-sector collaboration, sharing fraud insights, ensuring EU-level supervisory enforcement, and prioritizing consumer protection in product design. These recommendations are crucial for ongoing discussions on payment services regulation and emphasize the need for a comprehensive approach to combatting digital fraud beyond payment transactions.

Germany Unveils Draft Employee Data Act

On October 8, 2024, Germany's Federal Ministry of Labor and Social Affairs and the Federal Ministry of the Interior introduced a draft Employee Data Act. The act aims to modernize employee data protection by balancing company and employee interests in the digital workspace. It requires that any processing of employee data by employers or third parties be necessary for specific purposes and includes a necessity assessment to protect employees' rights and dignity.

PRIVACY DIGEST

Department for Science, Innovation, & Technology

UK Launches Regulatory Innovation Office to Boost Tech Market Entry

The UK's Department for Science, Innovation and Technology (DSIT) has established the Regulatory Innovation Office (RIO) to streamline regulations and accelerate market entry for emerging technologies, including AI in healthcare and delivery drones. The RIO aims to update regulations, expedite approvals, and improve collaboration among regulatory bodies. Initially, it will focus on sectors such as engineering biology, space, AI, and connected technologies in healthcare. The office integrates the functions of the Regulatory Horizons Council and the Regulators' Pioneer Fund within the DSIT.

DSIT Report: Cookie Consent Findings

A DSIT report published on September 4, 2024, revealed that most users accept cookies, with only 39% opting to decline them, even when default settings favor opting out. The study by the Behavioural Insights Team found that 42% of users want to customize their cookie settings, showing how design influences decisions. It highlights the 'privacy paradox,' where user actions contradict privacy intentions, and recommends browser-based, interactive cookie settings with clear information to align user choices with privacy preferences under GDPR.

ICO Launches New Data Protection Audit Framework

On October 7, 2024, the UK's Information Commissioner's Office (ICO) unveiled a new data protection audit framework to aid organizations in self-assessing compliance with data protection laws. This framework builds on the existing Accountability Framework and features nine toolkits covering areas like accountability, records management, cybersecurity, and AI. Each toolkit includes a downloadable audit tracker, enabling organizations to identify and address areas for improvement effectively.

ico.
Information Commissioner's Office

PRIVACY DIGEST

USA PRIVACY UPDATES

NYDFS Guidance on AI Cybersecurity Risks

On October 16, 2024, the New York State Department of Financial Services (NYDFS) issued guidance addressing cybersecurity risks associated with artificial intelligence (AI). The guidance clarifies that it does not introduce new obligations but helps entities comply with existing regulations. Key risks include AI-enabled social engineering, increased cyberattacks, and supply chain vulnerabilities. Recommended actions include updating cybersecurity programs, performing due diligence on third-party AI services, strengthening access controls, training staff, and effective data management. The NYDFS also emphasized that AI can enhance cybersecurity measures through improved threat detection and analysis.

AGs Sue TikTok for Harm to Children's Mental Health

On October 8, 2024, New York Attorney General Letitia James, alongside 13 other AGs, filed lawsuits against TikTok, accusing the platform of addicting young users, harming their mental health, and violating privacy laws. The lawsuits allege TikTok misled users about its safety, promoted dangerous challenges, and collected data from minors without consent. The AGs seek to impose financial penalties and force TikTok to change its practices to protect children from addictive features and privacy breaches.

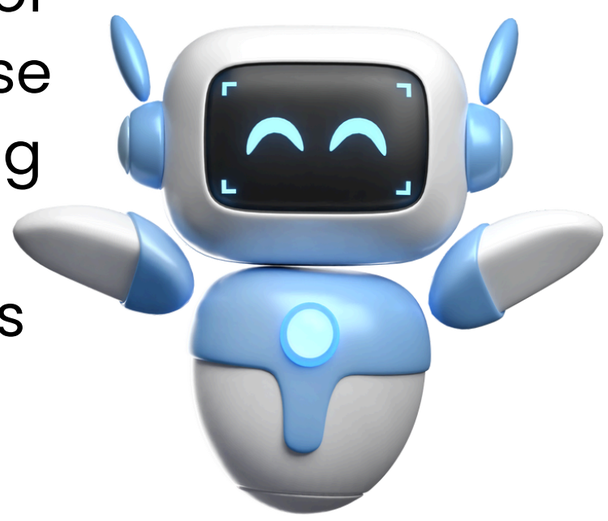
California's Senate Bill 976: Protecting Youth from Social Media Addiction

On September 20, 2024, Governor Gavin Newsom approved Senate Bill 976, the Protecting Youth From Social Media Addiction Act. The bill defines "addictive feed" and "addictive internet-based services" and sets conditions for displaying media without being classified as addictive. It prohibits social media platforms from providing addictive feeds to minors without verifiable parental consent and restricts sending notifications to minors during nighttime and school hours to help mitigate social media addiction in young users.

PRIVACY DIGEST

AI UPDATES

UNESCO and Colombia Partner on Ethical AI Use in Judiciary



On October 10, 2024, UNESCO and Colombia's Superior Council of the Judiciary announced a partnership to promote ethical AI use in the judicial system. This collaboration will focus on developing guidelines, building capacity, conducting algorithmic impact assessments, and sharing best practices to ensure AI enhances justice while respecting human rights. The initiative is part of UNESCO's broader effort to support responsible AI use globally, positioning Colombia as a leader in AI governance in Latin America. The project also aims to serve as a model for other countries.

Singapore Supreme Court Issues Circular on AI Use in Courts

On September 23, 2024, the Supreme Court of Singapore released Circular No. 1 of 2024, effective from October 1, outlining guidelines for the use of Generative AI in court proceedings. The circular applies to all court users, including lawyers and self-represented litigants. While AI tools are allowed for drafting documents, users must verify content for accuracy and ensure it adheres to intellectual property and confidentiality laws. AI cannot be used to generate evidence. Non-compliance may result in penalties, including cost orders or disciplinary action. The Court emphasizes user accountability for AI-generated output.

Malaysia Adopts National AI Governance and Ethics Guidelines

On 20 September 2024, Malaysia's Ministry of Science, Technology, and Innovation introduced the National Guidelines on AI Governance and Ethics. These voluntary guidelines encourage responsible AI usage among stakeholders like users, policymak and developers, emphasizing fairness, transparency, accountability, privacy, and inclusiveness. They align with global efforts from UNESCO, OECD, and the European Commission to promote ethical and trustworthy AI development.

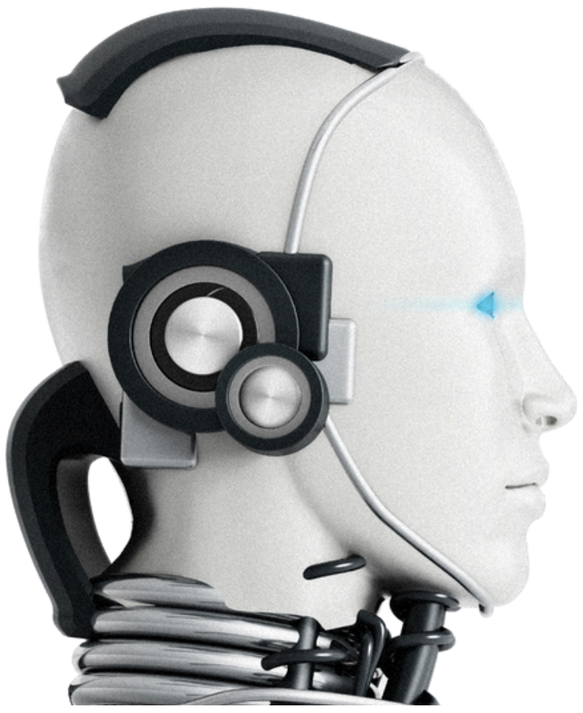
PRIVACY DIGEST

EDPB Stakeholder Event on AI Models – Express Your Interest

The European Data Protection Board (EDPB) is hosting a virtual stakeholder event on 5 November 2024 to gather input on AI models in relation to GDPR Article 64(2). Interested participants, including organizations, companies, and academics, are invited to express their interest. Registration will close once the maximum number of participants is reached. More details and registration instructions are available on the EDPB website.

Belgian Data Protection Authority Issues AI and Data Protection Guidelines

On 19 September 2024, the Belgian Data Protection Authority released guidelines on AI and data protection, focusing on the relationship between GDPR and the EU AI Act. The guidelines emphasize data protection principles like fairness, transparency, and accountability, particularly for high-risk AI systems. They also recommend bias mitigation, purpose limitation, human oversight, and a two-step risk management approach, with practical examples for implementation.



California Assembly Bill 2013 Enacted to Enhance Transparency in Generative AI

On September 28, 2024, California signed Assembly Bill 2013 into law, requiring developers to disclose comprehensive details about the training data used for generative AI systems or services offered to Californians since January 1, 2022. Key disclosures include data sources, purposes, copyright status, acquisition methods, and modifications made to the data. The law exempts AI systems utilized for security, national airspace operations, and national security. It also defines "substantial modification" as changes that materially impact the functionality or performance of the AI system.

PRIVACY DIGEST

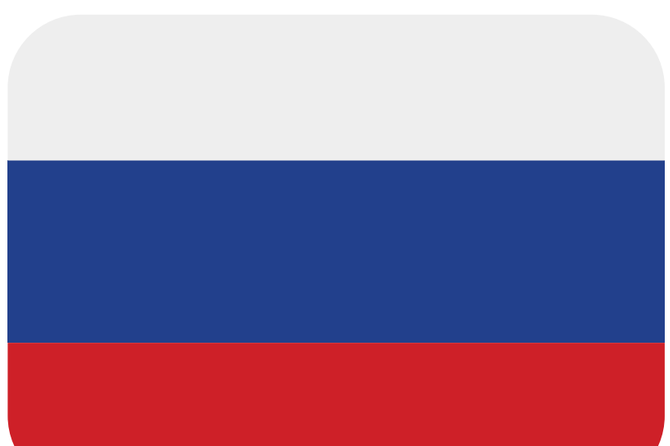
Instagram Introduces Teen Accounts with AI-Age Verification

On September 17, 2024, Instagram launched Teen Accounts, featuring privacy settings, content restrictions, and AI-driven age verification to enhance safety for users under 18. These accounts are private by default, limit messaging to known contacts, restrict sensitive content, and enforce screen time limits. Parental permission is required for teens under 16 to modify settings, while AI technology helps verify users' ages. The update follows scrutiny over Instagram's impact on teen mental health and is rolling out in several countries, with global implementation by January 2025

Artist Sues U.S. Copyright Office Over AI Art Rights

An artist, Jason Allen, has filed a lawsuit against the U.S. Copyright Office after it denied copyright protection for his AI-generated artwork "Théâtre D'opéra Spatial," created using the AI tool Midjourney. The Copyright Office argued that the work lacked human authorship. The case raises critical questions about copyright protection for AI-assisted art, including what constitutes enough human involvement for copyright eligibility. Allen contends that his extensive testing and refinement of AI prompts qualifies as significant creative effort, comparing his role to that of a director guiding a camera operator.

Russia's National AI Code of Ethics Gains Momentum with 820 Signatories



On September 18, 2024, Russia's National Center for Artificial Intelligence Development announced that 423 more organizations have signed the National AI Code of Ethics, bringing the total to 820 signatories. Developed by the AI Alliance and supported by the Ministry of Economic Development, the code outlines ethical standards for AI, including human-centered approaches, legal compliance, non-discrimination, and risk assessment. It emphasizes responsible data use, privacy, security, human oversight, and transparency throughout the AI system life cycle.

PRIVACY DIGEST

FINES AND PENALTIES

ICO Fines Service Box Group £40,000 for Unsolicited Calls

The Information Commissioner's Office (ICO) has fined Service Box Group Limited (SBG) £40,000 for making 5,361 unsolicited direct marketing calls to individuals registered on the Telephone Preference Service (TPS). This action violates the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). The fine follows an investigation that revealed SBG contacted TPS subscribers without their consent, contravening Regulation 21 of PECR.

OCR Fines Providence Medical Institute $240,000 for HIPAA Violations

On October 4, 2024, the U.S. Department of Health and Human Services' Office for Civil Rights imposed a $240,000 fine on Providence Medical Institute for HIPAA Security Rules violations. This penalty followed a ransomware attack that compromised the ePHI of 85,000 individuals. The OCR found unauthorized access and encryption of systems, inadequate technical policies, and a missing business associate agreement with the IT vendor during its investigation.

FCC Settles with T-Mobile for $15.75 Million Over Data Breaches

On October 1, 2024, the FCC reached a settlement with T-Mobile for $15.75 million related to data breaches in 2021, 2022, and 2023 that compromised customer personal and proprietary information. T-Mobile violated the Communications Act by failing to adequately protect customer data. As part of the settlement, T-Mobile will enhance its cybersecurity measures, including appointing a Chief Information Security Officer (CISO), adopting a zero-trust framework, implementing multifactor authentication, and conducting third-party security assessments.

PRIVACY DIGEST

Dutch DPA Fines Clearview AI for Illegal Data Collection

The Dutch DPA fined Clearview AI €30.5 million for illegally collecting billions of facial images, including those of Dutch citizens, without consent. Clearview's actions violate EU privacy laws (GDPR). The DPA warns that using Clearview's services is also illegal in the Netherlands, and organizations that do so may face additional fines. Clearview has not complied with previous penalties and may face further actions against its directors.

Meta Fined €91 Million by Irish DPC for GDPR Breaches

The Irish Data Protection Commissioner (DPC) has imposed a €91 million fine on Meta Platforms Ireland Limited for breaches of the GDPR stemming from improper password storage practices. In March 2019, Meta disclosed that user passwords were inadvertently stored in plaintext, prompting an inquiry into its GDPR compliance and security measures. The investigation revealed multiple violations, including inadequate security protocols and failure to notify and document the personal data breach.

Greek Ministry Fined €150,000 for GDPR Violations by HDPA

The Hellenic Data Protection Authority (HDPA) has fined the Ministry of Citizen Protection €150,000 for GDPR violations concerning the new Greek identity cards. The Ministry failed to adequately inform citizens about data processing and did not conduct a Data Protection Impact Assessment (DPIA) before handling biometric data. Following a complaint about the legality of the processing and the Ministry's delayed response, the HDPA imposed a €50,000 fine for information obligation violations and €100,000 for the lack of a DPIA. The Ministry is now required to align ID processing with European legislation and update the HDPA within six months.

PRIVACY DIGEST

ACMA Fines Commonwealth Bank for Spam Act Violations

The Australian Communications and Media Authority (ACMA) has fined the Commonwealth Bank of Australia (CBA) AUD 7.5 million for breaching the Spam Act. The bank sent over 170 million marketing emails without a functional unsubscribe option and 34.8 million emails to non-consenting customers between November 2022 and April 2024. This decision came after consumer complaints and an investigation into CBA's practices. Along with the fine, the bank must appoint an independent consultant to review and enhance its compliance with spam regulations and report back to the ACMA.

CNIL Fines COSMOSPACE €250,000 for GDPR Violations

The French data protection authority, CNIL, has imposed a €250,000 fine on COSMOSPACE for violations of GDPR and CPCE regulations. The company, which offers remote clairvoyance services via phone, chat, and SMS, was found to excessively record sensitive client data, retain it for six years despite claiming a five-year retention period, and process personal data without proper consent. Additionally, CNIL highlighted a lack of transparency regarding a shared database with TELEMAQUE, further compounding the violations.

South Korea Fines Worldcoin for Personal Data Violations

On September 25, 2024, South Korea's Personal Information Protection Commission (PIPC) fined the Worldcoin Foundation and its affiliate, Tools For Humanity, $829,000 for violating personal data protection laws. The fine followed an investigation into the collection of biometric data, such as iris scans, from nearly 30,000 South Koreans without proper consent or legal basis. The company failed to inform users about data transfer, retention, and deletion procedures. Despite the regulatory challenges, Worldcoin's native token surged 35% from $1.60 to $2.16 between September 19 and 26

PRIVACY DIGEST

DATA BREACH

Star Health Insurance Data Breach: 31 Million Customers' Data Exposed

Star Health Insurance experienced a massive data breach, compromising personal details of 31 million customers, including names, PAN numbers, and medical records. The hacker claims to have accessed 7.24TB of data and is offering it for sale online. Allegations against the company's CISO have been denied, with Star Health calling it a "malicious attack." The company is investigating, has filed a criminal complaint, and is working with authorities to protect customer data.

Casio Confirms Data Breach After Ransomware Attack

Casio has confirmed a data breach following a ransomware attack by the group Underground, which stole over 200 GB of data. Detected on October 5, the breach may have compromised personal information of employees, partners, and customers. As the hackers begin leaking data, Casio is working with police to protect affected individuals and urges against sharing the stolen information.

Internet Archive Data Breach Exposes 31 Million Users

The Internet Archive confirmed a data breach that compromised the information of 31 million users, including email addresses, usernames, and hashed passwords. Security researcher Troy Hunt verified the breach, which occurred in September, and added the data to his Have I Been Pwned database. The organization is also contending with ongoing DDoS attacks that have disrupted its services. Founder Brewster Kahle stated they are enhancing security measures while facing significant legal challenges over copyright issues.

PRIVACY DIGEST

Globe Life Extortion Attempt After Data Breach

Globe Life is facing extortion threats after hackers stole data from over 5,000 individuals linked to its subsidiary, American Income Life Insurance Company. The compromised information includes Social Security numbers and health-related data. While the company has notified federal authorities and is investigating, it reported that the threat actor has shared some stolen information with short sellers and attorneys. No ransomware or operational disruptions have occurred, and Globe Life is collaborating with cybersecurity experts to address the situation.

Omni Family Health Data Breach Investigation

Omni Family Health (OFH) has reported a data breach affecting thousands of patients and employees, linked to a cyberattack in February 2024. The breach may have exposed sensitive information, including names, Social Security numbers, and medical records. OFH began notifying impacted individuals on October 10, 2024. Levi & Korsinsky, LLP is investigating the breach to determine if affected individuals are entitled to compensation for potential identity theft and fraud. Those who received notification letters should check their eligibility for compensation.

PRIVACY DIGEST

"10 COMMON SCAMS TO AVOID AND STAY SAFE"

1	**TRAI Phone Scam:** Scammers claim TRAI will suspend your number for illegal activities—only telecom companies can suspend services.
2	**Parcel Stuck at Customs:** Fraudsters say a parcel with contraband is stuck and demand payment—report and disconnect.
3	**Digital Arrest:** Fake police officers threaten arrest online—this doesn't exist.
4	**Family Member Arrested:** Scammers demand money for a relative's release—verify with family first.
5	**Get Rich Quick Trading:** Ads promise high returns on investments—likely scams.
6	**Easy Money Tasks:** Offers of huge rewards for simple tasks often require upfront investments—avoid.
7	**Fake Credit Card Transactions**: Scammers claim transactions on a fake card—verify with your bank.
8	**Mistaken Money Transfers:** Scammers request refunds for supposed wrong transfers—confirm with your bank.
9	**KYC Expired:** Scammers request updates via links—KYC should be updated in person at the bank.
10	**Generous Tax Refund:** Fraudsters posing as tax officials ask for bank details—tax authorities don't ask this way.

Report Scams:

1. National Consumer Helpline (1800-11-4000)
2. Cyber Crime Reporting Portal (cybercrime.gov.in)
3. Local Police Station

Safety tips: Always verify information, don't click suspicious links, and report scams through official channels

Azure Data Protection Consultants LLP

Contact us for any queries:

https://azuredpc.com/

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com

DISCLAIMER