
Privacy Digest




AZURE DATA PROTECTION CONSULTANTS LLP

June 2024

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

PRIVACY DIGEST



Welcome to our June newsletter, where we focus on one of the most significant legislative developments in India this year – the Digital Personal Data Protection Act (DPDPA), 2023. This landmark piece of legislation was passed in August 2023 and it marks a new era for data privacy and protection in India. Recently, the Union Minister for Electronics and IT, Ashwini Vaishnaw, announced that the government will soon come up with a ‘digital design’ platform, showcasing that the implementation of the act is a priority for the Ministry and promising progress in the digital landscape of India.

For many years, India has been stagnating when it comes to enforcing strict privacy regulations. The absence of strong data protection laws has made India’s position comparatively weak in privacy landscape, which affects both individuals and businesses. However, implementation of DPDPA, 2023 can be said to be a game changer that will help make India more secure and privacy conscious aligning its standards with international best practices.

Another major impact that this act may have upon Indian data protection law relates to its potentiality of raising the profile of data privacy at an international level. Presently, India is not among the “adequate” third countries according to European Union thereby hindering easy transfer of data from EU countries. If DPDPA were implemented effectively then it will be a progressive step towards it.

As we move forward, the DPDPA, 2023 promises to bring about transformative changes, not only strengthening the privacy rights of individuals but also enhancing trust in digital services and platforms. This legislation is a vital step towards ensuring that India can compete and collaborate on a global scale, safeguarding personal data while enabling technological and economic growth.



Future of Data Privacy and Digital Legislation in India

Watch out this space for updates on upcoming India privacy legislation:

Digital Personal Data Protection Act (DPDPA)

Enacted in August 2023, the DPDPA aims to regulate data privacy. If the current government is re-elected, it pledges to operationalize this Act within the first 100 days. Key provisions include:

Consent Requirements: Explicit consent is required for data collection and processing.

Data Minimization: Only necessary data should be collected.

Rights of Data Subjects: Individuals can access, correct, and erase their data.

Data Breach Notifications: Companies must report breaches promptly.

Critics worry about the extensive powers granted to the government, which may lead to surveillance concerns.

Digital India Act

The Digital India Act aims to modernize digital service regulations. It will address data privacy, cybersecurity, and the regulation of emerging technologies like AI. Expected components include:

Data Protection Measures: Enhanced security for digital transactions.

Cybersecurity Frameworks: Guidelines to protect against cyber threats.

Technology Regulation: Rules for AI and blockchain, balancing innovation with ethics.
Implications

These laws aim to create a safer digital environment, but their success hinges on effective enforcement and balancing security with individual rights. Technology companies must adapt, and citizens should benefit from greater control over their data.



Protect Yourself from FedEx Scams: A Cybersecurity Alert

FedEx scams typically involve scammers impersonating FedEx employees or law enforcement officials to deceive individuals into believing they are involved in illegal activities. The scammers use various tactics, such as fake parcel seizures or threats of legal action, to coerce victims into transferring money or sharing sensitive information.

Recent Cases:

Bengaluru IT Firm CEO: A 66-year-old CEO lost Rs 2.3 crore to scammers claiming a parcel in his name contained illegal items.

Delhi Doctor: A 35-year-old doctor was coerced into transferring money during a three-hour video call with scammers posing as FedEx and police officers.

Bengaluru Lawyer: A lawyer was tricked into a compromising Skype call and extorted by scammers claiming a fake drugs parcel was sent in her name.

Bengaluru Businessman: A businessman lost Rs 1.98 crore to scammers pretending to be FedEx employees and law enforcement, alleging a package contained illegal drugs.

Delhi Woman: A 35-year-old woman transferred Rs 5.10 lakh to scammers posing as FedEx personnel and law enforcement officials.

Ways to Protect Yourself:

Verify Through Official Channels: Always verify the status of any FedEx package directly on the official FedEx website. Avoid clicking on links or engaging with suspicious communications.

Avoid Sharing Sensitive Information: Never disclose personal or confidential information to strangers, especially over the phone or online.

End Suspicious Calls Promptly: If a call raises suspicions, end it immediately without further engagement. Scammers often use psychological tactics to manipulate victims.

Be Aware of Law Enforcement Procedures: Legitimate law enforcement agencies do not conduct investigations or request payments through Skype calls. Verify through official channels and report any suspicious activity to the authorities.

Conclusion:

FedEx scams are a serious threat that can lead to financial losses and emotional distress. By staying vigilant, verifying information through official channels, and avoiding sharing sensitive information, individuals can protect themselves from falling victim to these fraudulent schemes. Awareness and caution are crucial in safeguarding against cyber-criminals.



BSE Implements Groundbreaking Encrypted Messaging System for Traders

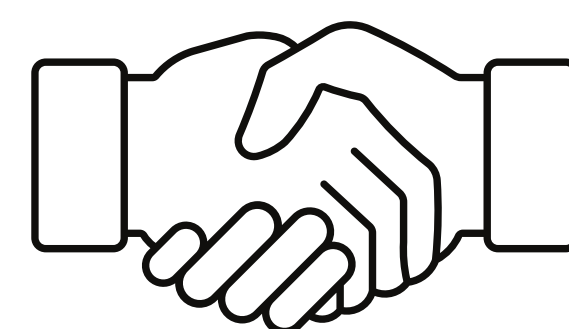
The Bombay Stock Exchange (BSE) has made headlines by becoming the first exchange globally to encrypt messages sent to traders. This pioneering move is aimed at enhancing security in the face of rising cyber threats. The encryption system, known as the "Encrypted Messaging System," ensures that all communications between the BSE and its trading members are secure and protected from unauthorized access. By implementing advanced cryptographic techniques, the BSE aims to safeguard sensitive information such as trade details, market insights, and client data. This initiative is part of a broader effort by Indian regulators and exchanges to fortify the country's financial infrastructure against cyber risks, demonstrating India's commitment to developing a strong and future-ready financial ecosystem.



UK PRIVACY UPDATES

Ofcom and ICO Announce Collaboration on Online Services Regulation

Ofcom and the Information Commissioner's Office (ICO) have issued a joint statement outlining their collaboration on regulating online services. Building upon a previous statement from 2022, this new agreement establishes clear plans for effective collaboration in identifying online safety and data protection issues. Key themes include collective approaches to age estimation and verification, proactive tech and AI tools, and upholding terms policies and community standards. Additionally, both organizations may share generic information about information requests relevant to online safety and data protection.



Information Commissioner's Office

ICO stated in response to Microsoft Recall Feature

With the recent hush among privacy advocates regarding the newly launched AI-powered "Recall" feature for Windows PCs which is designed to continuously store the screenshots of user's pc activity. ICO has initiated discussions with Microsoft to gain a comprehensive understanding of the measures in place to safeguard user privacy. ICO also indicates that organizations must consider data protection from the outset and rigorously assess and mitigate risks to people's rights and freedoms before bringing products to market.

Regarding the privacy practices of Recall, Microsoft justifies that: "To help maintain privacy, Recall processes the user content locally on the Copilot+ PC and securely stores it on the user's device only".

The Data Protection and Digital Information bill is technically dead

Several media outlets in the UK have speculated that the Data Protection and Digital Information Bill (DPDI) has been technically killed due to the lack of preparation time owing to the sudden dissolution of the UK parliament. The bill was intended to provide lenient procedures to access personal information for purposes such as law enforcement, health and social care etc.





Ofcom Unveils Draft Children's Online Safety Code of Practice

Ofcom, the UK's online safety regulator, has introduced a draft children's safety code of practice, comprising guidelines for user-to-user services and search services. For user-to-user services, measures include governance and accountability, assurance mechanisms, internal content moderation, and easy access to child protection terms. Search service obligations involve providing age-appropriate user support, managing predictive search suggestions, implementing content moderation, and ensuring accessible child protection terms.



New Cybersecurity Draft Codes Introduced in UK National Cyber Strategy

In line with the UK's £2.6 billion National Cyber Strategy, the Department of Science and Innovation has unveiled two new draft codes aimed at bolstering cybersecurity practices in AI systems. The first draft encompasses a voluntary code of practice, drawing from the National Cyber Security Centre's guidelines, to establish essential security standards for all AI technologies. Meanwhile, the second draft, titled the Code of Practice for Software Vendors, outlines 21 provisions across four core principles, delineating guidelines for software development, deployment, maintenance, and customer communication. These initiatives mark significant strides in enhancing online safety and resilience within the UK's digital landscape.



ICO Releases Guide: General Election and Your Personal Data

The Information Commissioner's Office (ICO) has unveiled a new information piece titled "The General Election and My Personal Data - What Should I Expect?" in a blog format. This guide outlines the rights of the public regarding the use of personal data by political parties, presented in a question-answer format. Divided into three sections, the guide covers expectations from political parties and campaigners, the role of the ICO, and what individuals can anticipate on Election Day



General election

My Personal Data



ICO has concluded their investigation on MY AI Chabot

ICO has concluded their investigation on Snapchat My AI Chabot about the concerns regarding the inadequate data protection compliance requirements surrounding the deployment of the said AI Chabot. The ICO executive director indicated a warning note that Organizations developing or using generative AI must consider data protection requirements, including rigorously assessing and mitigating risks to people's rights and freedoms before bringing products to market.

NEW ZEALAND PRIVACY UPDATES

Australian Information Commissioner Concludes TikTok Inquiry, Calls for Privacy Act Reforms

The office of the Australian Information Commissioner has closed the preliminary inquiries on TikTok. The inquiry revealed that there is no clear breach of Australian privacy law. The Privacy Commissioner also urged for urgent reforms of the Privacy Act to tackle the most harmful aspects of the digital ecosystem.





US PRIVACY UPDATES

US Securities and Exchange Commission has adopted rule amendments to “Regulation S-P”

The amendment was intended to modernize and enhance the rules that govern the treatment of consumers’ nonpublic personal information by certain financial institutions. The amendment requires the covered entities including but not limited to broker-dealers, funding portals, investment companies, registered investment advisers and transfer agents to:

Implement, develop and maintain formal procedures and written policies for incident response.

Shall notify the individuals about the data breach as soon as practicable, but not later than 30 days, after becoming aware of the incident.



FTC Enforces New Safeguard Rules for Data Breach Reporting

The FTC revised provisions for reporting data breaches and related incidents announced on October 2023 have come into force on May 13, 2024. The new rule titled “ Standards for safeguarding customer information” or simplify referred to as “ Safeguard rules ” mandates that non-banking financial institutions as soon as discovering a data breach affecting at least 500 customers shall be disclosed to FTC within 30 days after discovering the said breach.



Colorado Passed comprehensive AI act

Colorado governor has signed Senate bill 24- 205 into law thereby making Colorado the first US state to implement a full-fledged act governing artificial intelligence.

The act which is similar to the EU AI Act in applying a risk-based approach to regulating AI is set to take effect on February 1, 2026. The new act intended to focus exclusively on addressing bias and discrimination by implementing obligations for both deployers (who use AI systems to make decisions or assist in decision-making) and developers (who create or substantially modify AI systems). The act further defines High-risk AI systems, algorithmic discrimination consequential decisions etc.





California Assembly Passes Bill Requiring Opt-Out Preference Signals

The California assembly has recently passed the AB – 3048 bill that requires businesses to implement an opt-out preference signal under the rules adopted by the California Privacy Protection Agency. The bill specifically would prohibit companies from developing or maintaining web browsers that lack an opt-out preference setting.



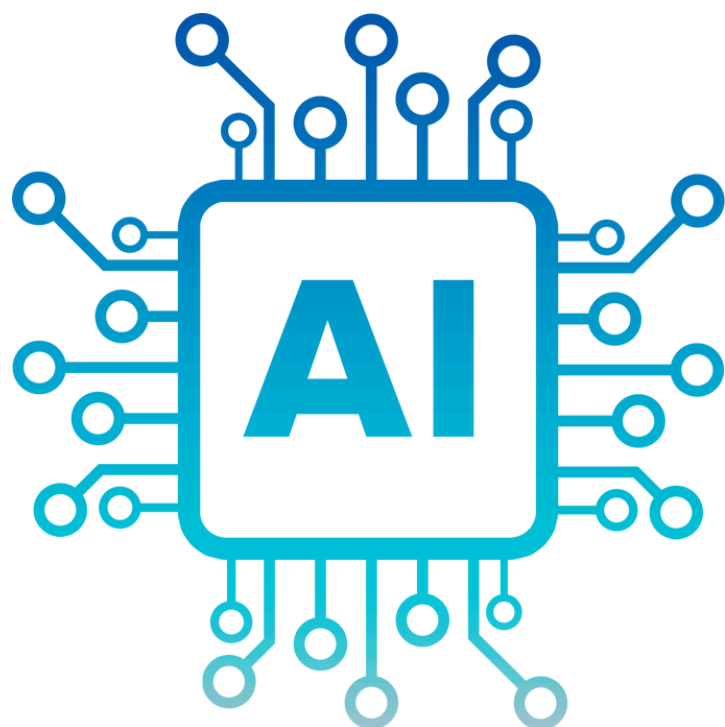
NIST

NIST Launches ARIA Program to Assess Societal Risks of AI

Marking the 180th day of the Executive order on trustworthy AI, the US National Institute of Standards and Technology (NIST) is launching a new testing, evaluation, validation and verification (TEVV) program known as Assessing Risks and impacts of AI (ARIA) intending to determine the societal risks and impacts of Artificial intelligence in a realistic setting. The ARIA expands on NIST AI RMF (risk management framework) will help develop quantifiable metrics and methodologies in determining how well a system maintains safe functionality within societal contexts.

Bipartisan AI Working Group Unveils Policy Roadmap

The US bipartisan AI working group has unveiled a comprehensive roadmap for artificial intelligence policy. Through nine bipartisan AI insight forums, including discussions on supporting US innovation, AI's impact on the workforce, and national security, the group has addressed key facets of AI implementation. Notably, in the realm of privacy and liability, the group advocates for a robust federal data privacy law. This proposed legislation would encompass principles such as data minimization, security, consumer rights, consent, disclosure, and regulation of data brokers.





Vermont Passes Stringent Privacy Law: Key Provisions and Implications

Vermont recently passed one of the strictest privacy laws in the USA, pending the governor's assent. This comprehensive legislation includes provisions for a private right to action against companies collecting data from over 100,000 individuals annually. Additionally, the law mandates the establishment of an Artificial Intelligence and Data Privacy Advisory Council to advise the government on AI use, prohibits the sale of sensitive personal data, and sets strict timelines for controllers to respond to data subject requests.



NEW ZEALAND PRIVACY



Privacy Commissioner
Te Mana Mātāpono Matatapu

New Zealand Privacy Commissioner's Office Issues Guidelines on Data Breach Reporting Time frames

The New Zealand Privacy Commissioner's Office has issued guidance on the time frame for informing the privacy commissioner about the data breach. The guideline titled "How long is 72 hours" explains the term what it means by 72 hours and encourages the controllers to make use of the "our notify us tool" to assess how serious is the breach and whether it is mandatory to notify the privacy commissioner. The guide further defines the term "becoming aware" and encourages the controllers to update regularly on the recurring information about the incident on an incremental basis.

Call for Submissions: Privacy Amendment Bill Introduces IPP 3A

The Chairperson of the Justice Committee invites submissions on the Privacy Amendment Bill, which proposes changes to the Privacy Act 2020. Notably, the bill introduces IPP 3A, requiring entities collecting personal information indirectly to disclose details such as the purpose of collection, intended recipients, and agency information to the individuals concerned. This transparency initiative aims to bolster privacy protections and empower individuals regarding their personal data.





Privacy Commissioner Releases 2024 Survey

Findings: Shifts in Awareness and Behavior Emerge

The privacy commissioner has published the results of the 2024 bi-annual survey on privacy. The survey is intended to measure awareness, knowledge and levels of concern regarding privacy and protection of personal information. The key results of the survey include:

- Total concern for individual privacy has risen to 51%.
- The most common things people avoided doing in the past 12 months due to privacy concerns were:
 - Social media (33%)
 - Online browsing (28%)
 - Online shopping (28%) and
 - Online dating (28%).
- There was an increase in those likely to change service providers in response to poor privacy and security practices with 70% declaring they were likely to consider changing service providers.



EU PRIVACY UPDATES



European Data Protection Board

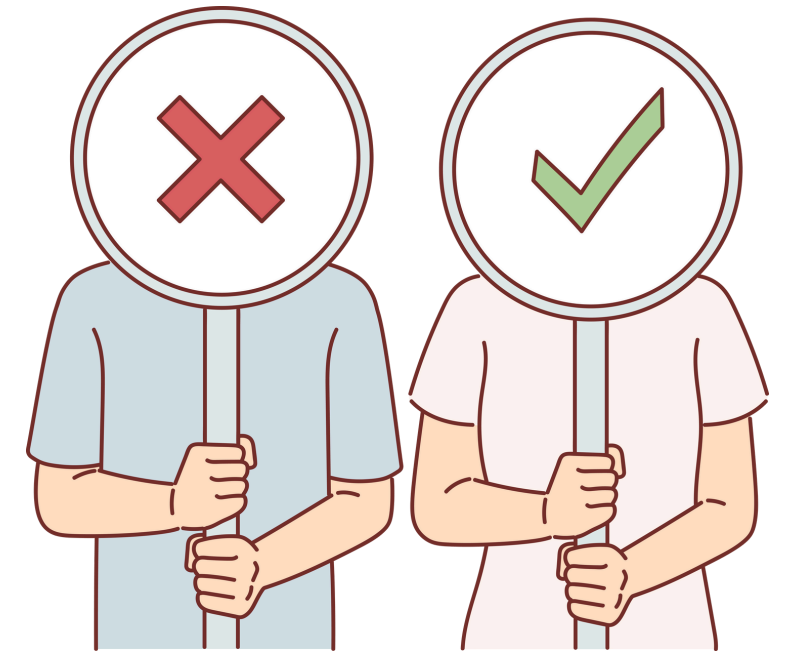
EDPB Releases Preliminary Report on Taskforce ChatGPT's Investigations

EDPB has published a preliminary report on the work of Taskforce ChatGPT. The task force which was set up last year has now produced a report which contains the initial conclusions from the investigations carried out by several European supervisors. The report distinguishes the data collection of chatGPT into training, prompts, preprocessing of personal data, output and training of chatbot with its prompts. The task force awaits the results of other supervisory authorities for its final decision.



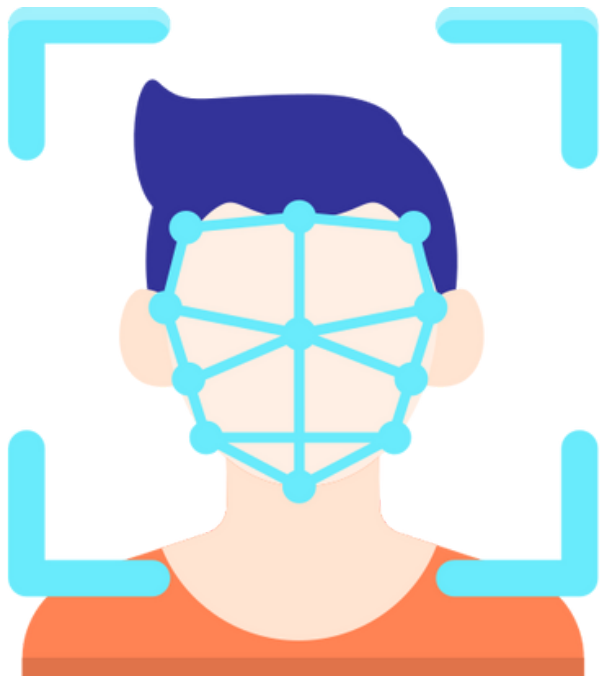
EDPB to Develop Guidelines for Consent or Pay Models

EDPB has decided to frame guidelines for the deployment of consent or pay models. The board decided that the said guidelines will be framed based on its consent or pay opinion published on 17 April 2024 and intended to analyze its impact on minors, its compliance with the privacy directive etc.



Compliance Guidelines for Airport Facial Recognition

With the request from the French data protection authority, EDPB has issued an opinion on the use of FRT by airport operators and airline companies. The opinion indicates several key compliance requirements including that the said entities shall justify the impossibility of deploying other less intrusive methods before using FRTs, only the biometric data of passengers who actively provide consent shall be processed, the storage solutions shall be compatible with the integrity and confidentiality principle, data protection by design and default principles of GDPR.



EDPB Launches Multilingual GDPR Guide for Small Businesses

EDPB has launched a Data protection guide for small businesses that covers most of the aspects of GDPR in French and German versions. Shortly, EDPB observes that the Guide will become available in 15 more European languages.





IRELAND PRIVACY UPDATES

The Irish Data Protection Commission has published its Annual report for 2023

The Annual report of 2023 highlights:

- 1.5 billion euro fine levied on tech giants including tik tok and meta
- Administrative fines were levied on five different organizations including the Bank of Ireland, Centric Health etc.
- The DPC received 25,130 electronic contacts 2,7,085 phone calls and 1,253 postal contacts.
- The total number of valid breach notifications received in 2023 was 6,991 and 92% of them were concluded by year-end.
- DPC provided input and observations on over 37 pieces of proposed legislation.



**An Coimisiún um
Chosaint Sonraí**
Data Protection
Commission

The DPC has launched a formal inquiry into the HSE

The Data Protection Commission has launched a formal inquiry into Health service executive (HSE) after videos surfaced online showcasing the alleged unauthorized access of personal data stored in paper records in external facilities. The DPC confirmed that the paper records in external storage facilities and breaches of security were notified to the DPC. The spokesperson of HSE reiterated that their organization will take all data breaches seriously in line with the data protection legislation and its internal policy.



Feidhmeannas Seirbhíse Sláinte
Health Service Executive

Data Protection Commission successful in defending their convictions.

The DPC has successfully prosecuted two companies for sending unsolicited marketing communications without consent. The Dublin Metropolitan District Court has levied fines for both companies thereby confirming the alleged violation. The chairperson of DPC commented that the companies offering marketing emails shall ensure that they have valid up-to-date consent of individuals and fully functioning opt-out mechanisms for the same.





SPAIN PRIVACY UPDATES

Guideline Highlights DPIA Need for Wi-Fi Tracking and AI Integration

The guideline addresses the technical and legal implications of Wi-Fi tracking technology, emphasizing the necessity of Data Protection Impact Assessments (DPIAs) for most deployments. It points out that under GDPR Article 35(3), processes involving Wi-Fi tracking in publicly accessible areas mandate DPIAs due to the technology's inherent complexities. Even if large-scale processing isn't intended, the guideline underscores the need for DPIAs in every instance due to potential challenges in individuals exercising their rights. Additionally, it advocates a balanced approach for complying with AI regulations, especially when combining Wi-Fi tracking with AI systems.



Spanish DPA Introduces Free GDPR Management Tool

The Spanish Data Protection Authority (DPA) has launched Gestiona RGPD/Manage GDPR, a free tool aimed at assisting controllers, processors, and DPOs in managing GDPR compliance. This tool provides guidance on handling Records of Processing Activities and initiating risk analysis. However, it's important to note that while the tool offers support, it does not replace accountability or limit decision-making power, with its reports intended only as supplementary documents.

Spanish Data Protection Authority Temporarily Halts Meta's Voter Information Features

The Spanish data protection authority, AEPD, has imposed a 3-month ban on Meta's Election Day Information and Voter Information Unit features, citing concerns about violating data protection principles. AEPD highlights potential issues such as heightened profiling, intrusive processing of sensitive data, and the risk of undisclosed parties accessing personal information for unspecified purposes.





Catalan DPA Reports Surge in Complaint

The Catalan Data Protection Authority (APDCAT) received 843 complaints in 2023 which indicates an increase of almost 37% compared to the previous year. The authority observes that regarding sanctioning procedures, it has initiated a total of 293 preliminary investigation actions in 2023. Of these, 87 have ended with a resolution, including reprimands, financial sanctions and suspensions.

The authority indicates that such a rapid increase in complaints is due to the increased awareness among data subjects.

Catalan DPA Implements Compliance Action on GDPR Right to Access

The Catalan Data Protection Authority (APDCAT) has initiated a coordinated compliance framework action as promoted by EDPB to provide updated information on the degree of compliance with the right to access as mentioned in GDPR. As a part of the action, it has launched a survey of public entities in Catalonia. The survey intended to address the number of registered access requests and the percentage they represent concerning the rest of data protection rights (rectification, deletion, etc.).



DENMARK PRIVACY UPDATES

Danish DPO Launches AI and Compliance Impact Templates

The Danish DPO has launched two new templates for carrying out impact assessment including one for AI systems and the other one is a generic template with updated compliance requirements.

The Template for AI assessment has been drafted by taking inspiration from the ICO AI and data protection risk tool kit. The template incorporates a risk management framework with a precaution that the catalogue of risks and measures is not exhaustive.

Both templates are currently not available in English.



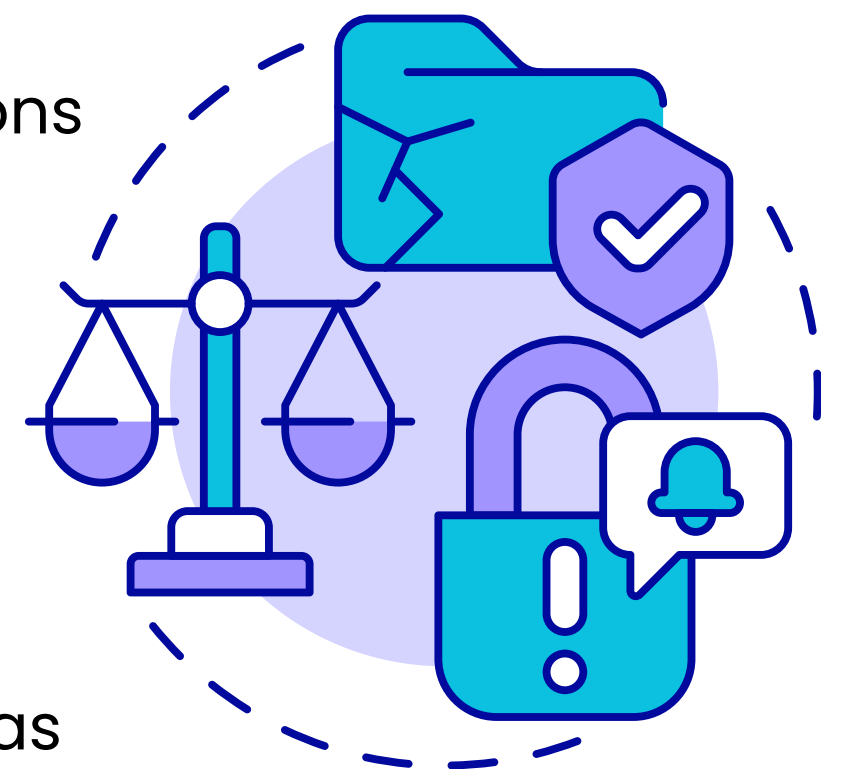


Danish DPA Issues Guidelines on Data Breach

Notification to Subjects

The Danish DPA has introduced new guidance on the requirements of data breach notification to data subjects. The guidance was drafted based on the inspection conducted on various corporations operating in Denmark and concluded that the data breach notification to the data subjects shall essentially contain all the relevant information including

- description of the nature of the breach in clear and understandable language,
- description of the likely consequences of the breach
- description of the measures that the data controller himself has taken or
- recommendations to reduce possible harmful effects of the breach
- Any other information that enables the data subjects to take necessary precautions to safeguard their rights.



FRANCE PRIVACY UPDATES

CNIL's New Guidelines on Athletes'

Disability Data

CNIL has issued guidance on collecting data regarding athletes' disabilities. It states that any data identifying disability falls under sensitive health data. Controllers must justify data collection for specific uses like licensing or safety measures and identify a legal basis such as consent or contractual obligation.

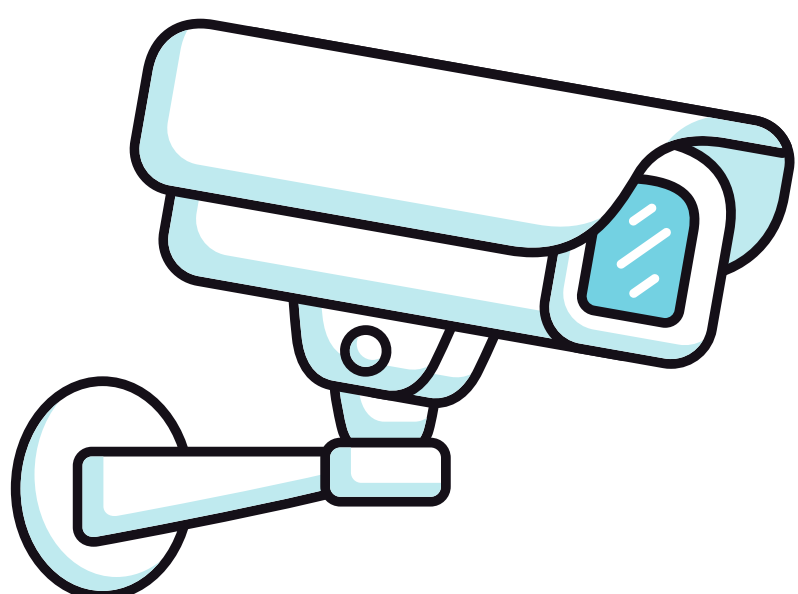


CNIL Releases Guidelines for Video Surveillance in Nursing Homes

Following the recommendation in public consultation, the CNIL has released guidance for the installation of video surveillance devices in nursing homes.

The guidance indicated that the installation of video surveillance devices shall only be justified in special circumstances including:

- In the event of a substantiated suspicion of mistreatment and
- Failure of investigation procedures which have not made it possible to detect a situation of mistreatment, when doubt remains.
- Before deployment, mandatory DPIA shall be conducted.





ASIA PRIVACY UPDATES



Privacy Commissioner Condemns World Coin's Data Practices

Honking: The office of the privacy commissioner for personal data, has found that the operation of World Coin violates the provisions of the personal data (privacy) ordinance. The investigation observes that:

- The biometric data collection of world coin is unnecessary, excessive and carried out without privacy notice and biometric data consent form in Chinese language.
- The data retention period of 10 years to train AI models for the user verification process is considered as too long and amounts to prolonged retention of personal data.
- Participants did not have the means to exercise their rights to data access and correction.
- World Coin failed to inform the participants about the possible risks of the disclosure of biometric data.

DATA BREACH



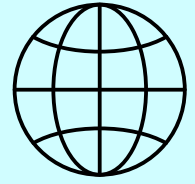
BBC Data Breach: Insights and Response Measures

BBC recently experienced a data breach affecting 25,000 current and former employees. While the nature of the breach remains undisclosed, BBC promptly informed affected individuals and regulatory authorities. They provided detailed FAQs and personally contacted those affected, showcasing a proactive response. However, caution is advised in such communications to avoid causing unnecessary panic and potential data protection violations.



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.