# Privacy Digest


AZURE DATA PROTECTION CONSULTANTS LLP

APRIL 2024

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

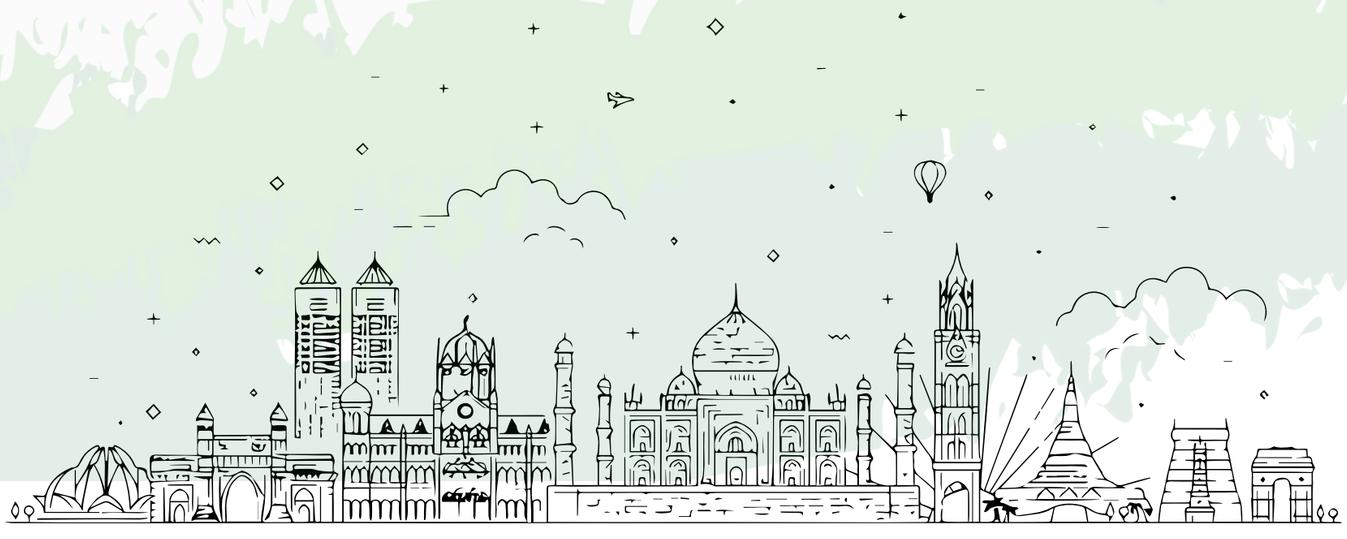
APRIL 2024 AZURE DATA PROTECTION CONSULTANTS LLP

# PRIVACY DIGEST

## Latest Trends

### FIRST THING FIRST. LETS REVIEW THE CONSENT MANAGEMENT FRAMEWORK

India's Digital Personal Data Protection Act, 2023 (the "DPDP Act") is a major advancement in safeguarding the security and privacy of peoples' personal data. The Consent Manager Framework, which might completely alter how personal data is gathered, processed, and managed, is the main idea behind the law. This creative method seeks to strike a balance between giving people more control over their personal data and giving organizations the direction and resources they need to successfully negotiate the tricky terrain of data security and privacy.



# PRIVACY DIGEST

# CONSENT FRAMEWORK UNDER DPDPA 2023

## WHAT CONSTITUTES AS A CONSENT MANAGER UNDER THE DPDP ACT?

A person/ entity who is registered with the Data Protection Board of India and serves as a single point of contact for data principals to grant, manage, evaluate, and revoke consent via an easily accessible, transparent, and interoperable platform is known as a consent manager under the Act. Through a consent manager, a data principal may review, provide, manage, evaluate, or revoke their consent to the data fiduciary. The consent manager represents the data principal and is answerable to them. The Government will then specify in the regulations the scope of this accountability. Additionally, the consent manager may be contacted by the data principal to seek grievance resolution and to exercise their rights under the Act.

Presently, the Act lacks additional elucidation regarding the responsibilities of consent managers; nevertheless, it stipulates that the Government will promulgate rules and regulations pursuant to the Act, which will expound upon the process of registration, prerequisites for registration, liability, and consent manager obligations.

## PRECEDING INITIATIVES FOR CONSENT MANAGEMENT

Before the DPDPA, India had initiatives like the Account Aggregator (AA) Framework and the NITI Ayog's Data Empowerment and Protection Architecture (DEPA) draft policy, which laid the foundation for consent management. The AA Framework allowed data exchange with regulated entities via a data-blind intermediary, while DEPA envisioned "consent managers" facilitating data flow based on user consent. These initiatives are likely to inform the development of the DPDPA's consent management system.

# PRIVACY DIGEST

## PRIVACY UPDATES

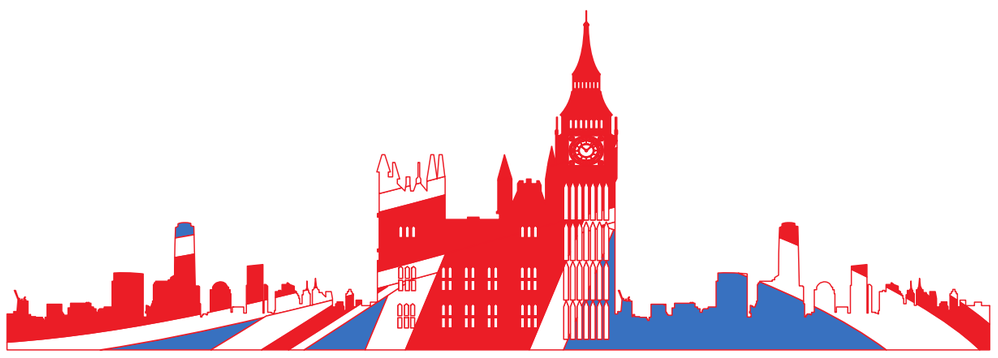
Information Commissioner's Office

### ICO's New Data Protection Fining Guidance: Key Highlights

The Information Commissioner's Office (ICO) has published new data protection fining guidance, replacing the penalty notices section in the regulatory action policy from November 2018. The guidance outlines circumstances for issuing penalty notices, factors considered in determining fines, approach to fines for multiple infringements, and assessment criteria including seriousness, nature, gravity, intentionality, and duration of the infringement. It also includes a five-step process for calculating fines, involving assessment of infringement seriousness, consideration of turnover, calculation of starting point, adjustment for aggravating or mitigating factors, and evaluation of fine effectiveness, proportionality, and deterrence.

### ICO Initiates Call for Views on "Consent or Pay" Business Models

The ICO has opened a call for views on "consent or pay" business models, reflecting its stance on online advertising. This initiative aims to evaluate how organizations prioritize users' interests, rights, and freedoms. Key aspects include ensuring users are fully aware of interactions with online services, making informed and voluntary choices, presenting choices equitably, ensuring equivalence between ad-funded and paid-for services, and justifying fees objectively.



# PRIVACY DIGEST

## ICO Issues Guidance on Information Sharing in Mental Health Emergencies at Work

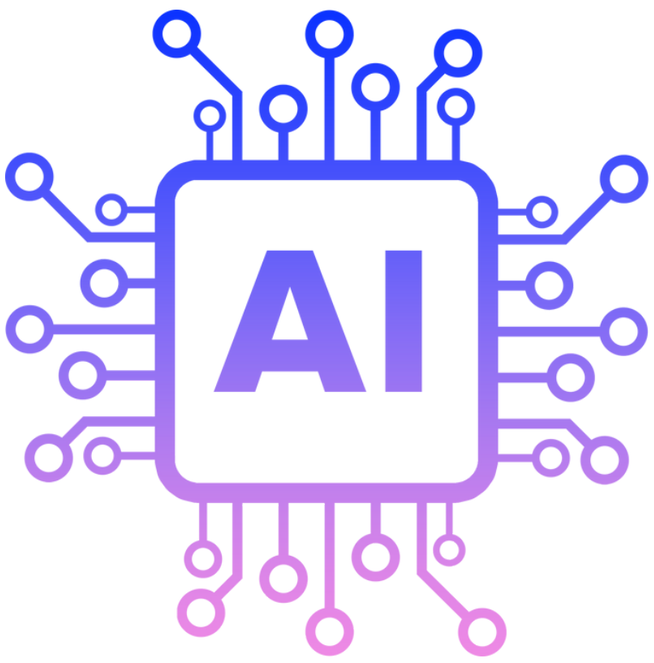
The ICO has released new guidance regarding information sharing in mental health emergencies at work, which complements existing guidance on processing workers' health information. This guidance advises employers on when and how to appropriately share workers' information if they believe someone is at risk of causing serious harm to themselves or others due to their mental health. Key recommendations include limiting information sharing to relevant parties such as emergency services or health professionals, informing workers about potential information sharing in health emergencies, conducting a Data Protection Impact Assessment (DPIA), developing a policy on sharing personal information in mental health emergencies, training staff on handling personal information in such situations, and obtaining separate emergency contacts for general and mental health emergencies on an emergency contact form.

## 4. ICO AND G7 DATA PROTECTION AUTHORITY HAS PUBLISHED A STUDY ON PRIVACY-ENHANCING TECHNOLOGIES.

the guide focuses on how synthetic data, generated from a real medical prescription dataset, can be used as part of a testing strategy for the development of a healthcare planning and resource allocation system, without the need to share sensitive patient information. The study concludes that without the need for real patient data, it can enable the decision makers to make more targeted decisions for effectively meeting local needs.

APRIL 2024 AZURE DATA PROTECTION CONSULTANTS LLP

# PRIVACY DIGEST

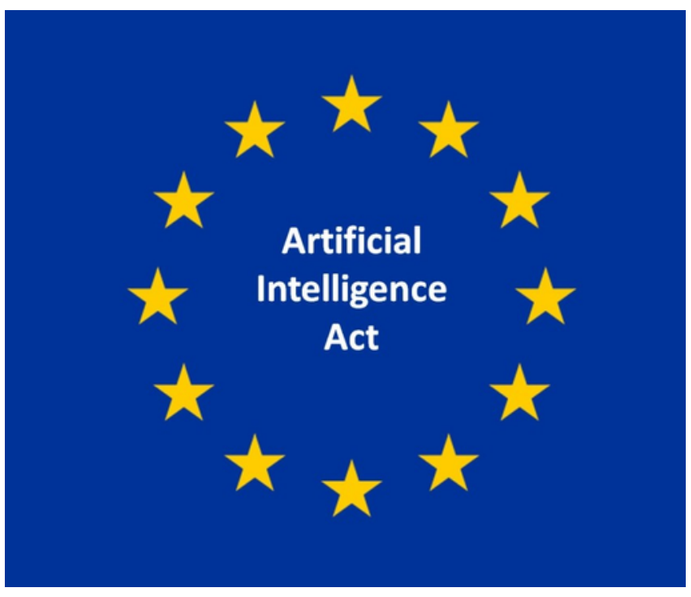



## UK AI Regulation Bill Receives Mixed Reactions

The UK AI Regulation Bill, presented by Lord Holmes, has successfully passed its second reading in the House of Lords. The bill aims to establish a national AI authority, introduce a regulatory sandbox for AI, and mandate companies to appoint an AI-responsible officer. However, reactions from policy experts are mixed. Some argue that the bill's strong focus on risk mitigation may stifle innovation, while others contend that such an approach is essential for fostering innovation in AI.

## Uber Eats Driver Wins Settlement in Facial Recognition Case

Uber Eats driver in the UK wins financial settlement due to facial recognition technology discrimination. Despite repeated failures of the FRT system to recognize him, he was removed from the platform. With support from EHRC and ADCU funding, he highlights dangers of AI misuse and lack of recourse. Final hearing set for Nov 2024.




## EU Parliament Approves Historic Artificial Intelligence Act

The EU Parliament has overwhelmingly approved the groundbreaking Artificial Intelligence Act, with 523 votes in favor, 46 against, and 49 abstentions. The Act aims to implement a risk-based approach to protect fundamental rights, the rule of law, democracy, and environmental sustainability from high-risk AI. Key highlights include conditions to verify decision correctness, measures to hold individuals accountable for incorrect decisions, classification of AI systems based on risk factors, prohibition of certain manipulative AI practices, and potential fines of up to 7% of the entity's global annual turnover for non-compliance.

# PRIVACY DIGEST

## AEPD ORDERS A BAN ON WORLD COIN BIOMETRIC DATA COLLECTION FOR 3 MONTHS DUE TO PRIVACY CONCERNS.

AEPD observes that based on the several complaints received against the company regarding the collection of data from minors and the fact that consent cannot be withdrawn, insufficient information about the company's operations it has ordered a precautionary measure against the company to cease the collection and processing of personal data being carrying out in Spain to avoid potentially irreparable damage.

## AEPD PUBLISHED A GUIDANCE BLOG ON THE EVALUATION OF HUMAN INTERVENTION IN AUTOMATED DECISIONS.

AEPD published a framework stressing the importance of meaningful human intervention in the various stages of an automated decision. For a systematic implementation of this intervention, the key criteria shall include competence and authority, preparation and training, capacity to alter the automated decision, and Means and resources to be able to exercise their competence and qualification.

# PRIVACY DIGEST

## GARANTE HAS LAUNCHED AN INVESTIGATION AGAINST OPEN AI'S SORA.

OpenAI SORA

The Italian data protection authority with no specific accusations about privacy violations has decided to examine the potential implications of Open AI's video generation platform Sora AI. As a part of its investigation, Garante has made a formal request to Open AI to disclose information regarding the training algorithm, the current availability of the service in the EU or Italy, the data collected and used for training etc.

DATATILSYNET

## THE DANISH DATA PROTECTION AUTHORITY IN COLLABORATION WITH THE DANISH AGENCY FOR DIGITALIZATION HAS INTRODUCED A REGULATORY SANDBOX FOR AI.

This regulatory sandbox is intended to provide free access to companies and authorities to relevant expertise and guidance on the applicable legal framework i.e. GDPR and its impact on the business, Strengthened perception of the company or authority as responsible and proactive in the approach to ethical and responsible use of AI and ultimately reducing the time between development to operation between new AI solutions. The deadline for applications for a sandbox course in 2024 is 21 May 2024.

# PRIVACY DIGEST

## DANISH AGENCY REPORT ON DATA PASSING TO TECH GIANTS.

A Danish digital agency examined 24 free games targeting children and young people and observed that irrespective of the creation of a profile or not these games have been sending personal data to large tech giants including Facebook, google and TikTok. Despite the efforts to prohibit tracking the apps have transferred data to the third-party platform. The report concludes that Facebook collects data via all 24 games examined, while Google and the company AppLovin collect data from almost all (95 per cent) of the game apps examined. TikTok collects data from 40 per cent of the analyzed games.

## LATVIAN DATA PROTECTION AUTHORITY DATU VALSTS INSPEKCIJA HAS PUBLISHED A 3 SERIES OF GUIDANCE ON PROCESSING PERSONAL DATA IN SPORTS COMPETITIONS.

Data State Inspectorate Republic of Latvia

The guidance indicates that the sports organizers shall handle personal information by following the below principles including:

- Obtaining consent before publishing results
- Pseudonymisation of participants' data
- Ensure principles of good governance
- Disclosure of personal information shall be based on a balanced approach between the legal basis for disclosure and the scope of the athlete’s professional activity.

# PRIVACY DIGEST

## THE KENTUCKY SENATE UNANIMOUSLY PASSED THE KENTUCKY CONSUMER DATA PROTECTION ACT.

The act which is an adaption of the Virginia privacy law does not impose major requirements on companies. With a serious business-friendly intent, it retains certain key provisions including conducting DPAI for certain higher-risk data processing activities (including targeted advertising, sale, profiling, and processing of sensitive data), obtaining consumer consent before processing sensitive data and a penalty up to 7550 dollars for each continued violation can be levied.

The effective date is 1, Jan 2026.

## FTC Releases 2023 Privacy and Data Security Update.

The Federal Trade Commission released its Privacy and Data Security Update for 2023 highlighting its accomplishments in the past three years in the areas of privacy and data security. The report summarizes all the FTC decisions on every company on the various issues ranging from AI, children and teen privacy, sensitive data and its rule-making initiatives to establish sensible and reasonable baselines that protect consumers and put honest businesses on a level playing field and geolocation data violations.

# PRIVACY DIGEST


## NEW YORK IMPLEMENTS SOCIAL MEDIA PRIVACY REGULATIONS

Starting March 12, 2024, New York will enforce Assembly Bill (A) 00836 and Senate Bill (S) 021518A, prohibiting employers from requesting employees' or job applicants' social media login credentials. Employers cannot deny employment solely based on refusal to disclose personal social media accounts. However, employers can require access to non-personal company accounts, access publicly available information, comply with court orders, and restrict employee access to certain websites via company devices or networks.

## DOT Privacy Review: Safeguarding Passenger Data

The U.S. Department of Transportation is reviewing the ten largest airlines to ensure they handle passengers' personal data properly. This includes examining their data collection policies, advertising practices, employee training, and any potential unfair or deceptive data sharing. The review is carried out under COPPA, with possible enforcement actions for violations.

# PRIVACY DIGEST

## UTAH UPDATED DATA BREACH NOTIFICATION REQUIREMENTS.

Utah lawmakers have updated the Utah Protection of Personal Information Act and the Utah Technology Governance Act inserting new definitions and requirements for data breach notifications to the Utah cyber center.


The amendment mandates the government entity to notify the Utah cyber centre as soon as practicable when the governmental entity becomes aware of a data breach.

The notification shall comprise of:

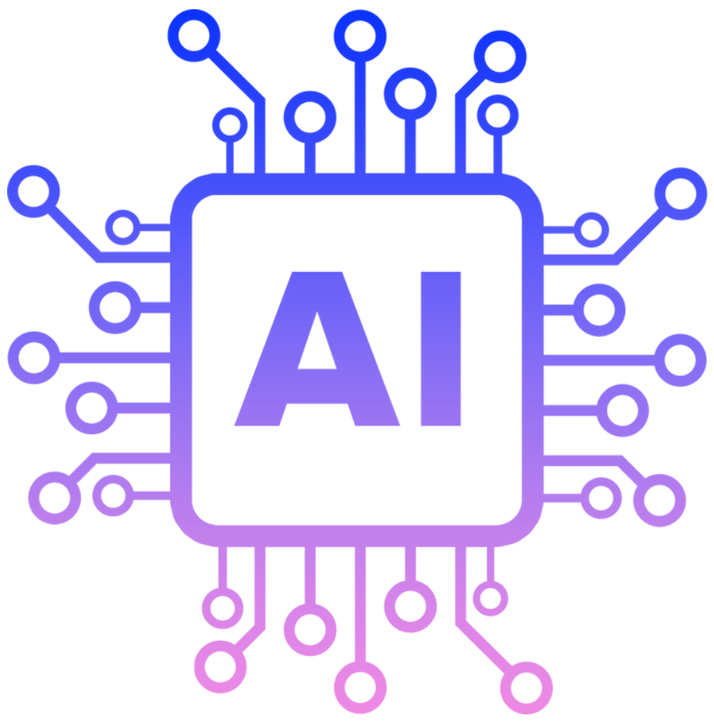
- Date and time of the breach occurred and discovered.
- Total no of people affected including a separate indication of no of persons based in Utah.
- type of personal data involved
- short description of the data breach
- path or means by which access was gained to the system, computer, or network (if known)
- individual or entity who perpetrated the data breach, (if known)
- steps taken to mitigate the impact of the data breach

## Protecting Americans' Data from Foreign Adversaries Act 2024"

The Protecting Americans' Data from Foreign Adversaries Act 2024 prohibits data brokers from selling sensitive information of US residents to countries like China, Iran, North Korea, Cuba, Russia, and Venezuela's Maduro government. Violations can lead to fines of up to $50,000, enforced by the FTC. Data brokers are defined as entities selling or transferring data they didn't collect directly from individuals, excluding service providers.

# PRIVACY DIGEST

## CALIFORNIA GOVERNMENT LAUNCHES GENAI GUIDANCE FOR THE PUBLIC SECTOR.




Under the executive order N-12-23 on Gen AI the newly introduced guidelines provide the necessary information and steps for state leaders to assess responsibly and accurately – and potentially procure and deploy – GenAI tools in their state entity. The guidance mandates all the state agencies to designate an employee responsible for monitoring GenAI tools, carrying out assessment and risk evaluation etc. and all the government workers are expected to receive meaningful training on AI and the best practices to prevent discrimination.

## FTC Public Consultation: Extending Liability for Impersonation in Trade Regulations

The FTC has initiated a public consultation for proposed amendments to trade regulations concerning the impersonation of government entities. Following recommendations from consumer and privacy advocacy groups, the proposed rule aims to include impersonations of individuals and hold entities accountable, including suppliers of AI tools, if they are aware that these tools will be used for unlawful impersonations. The public consultation period concludes on April 30, 2024.

## US Introduces Federal AI Governance and Transparency Act

The Federal AI Governance and Transparency Act (HR 7532) introduced by the US House of Representatives regulates AI systems in the federal government, focusing on transparency, accountability, and compliance. It mandates that AI use serves the public interest and avoids unjust harm or benefit to individuals or groups.

# PRIVACY DIGEST

## UN Resolution: Promoting Safe and Ethical AI Development

The UN has adopted a resolution promoting safe, secure, and trustworthy AI, co-sponsored by over 120 member states. It acknowledges AI's potential in nonmilitary sectors and emphasizes principles like human-centricity, reliability, explainability, ethics, inclusivity, respect for human rights and international law, privacy preservation, and sustainability. The resolution aims to tackle improper or malicious AI use, bridge digital divides, and align AI development with the UN's 17 sustainable development goals.

## OECD Updates Definition of AI: Explanatory Memorandum Released

The OECD has revised its definition of AI, originally outlined in the 2019 OECD Recommendation on AI. The updated definition describes an AI system as a machine-based system that infers outputs from inputs to influence physical or virtual environments, with varying levels of autonomy and adaptiveness post-deployment. The OECD has released an explanatory memorandum detailing the rationale behind the updated terminology.

## Mexico Introduces Federal AI Regulation Bill

Mexico proposes a Federal Law Regulating Artificial Intelligence, inspired by the EU AI Act. It categorizes AI into unacceptable, high, and low risk, with specific mitigation requirements. The law aims to have extraterritorial effects on AI service providers affecting Mexico and designates the Federal Telecommunications Institute (IFT) as the main regulatory authority. Penalties for non-compliance can reach up to 10% of a company's annual income.

APRIL 2024 — AZURE DATA PROTECTION CONSULTANTS LLP

# PRIVACY DIGEST

## CHINA EASES CROSS-BORDER DATA TRANSFER RULES: NEW REGULATIONS SUMMARY

China's Cyberspace Administration issues regulations easing cross-border data transfer rules, exempting companies from pre-conditions under the Personal Information Protection Law. Exemptions include data collected for international trade, contractual necessity, employee management, and emergencies concerning life, health, or safety.

## PDPC HAS RELEASED ADVISORY GUIDELINES ON THE PDPA FOR CHILDREN'S DATA IN THE DIGITAL ENVIRONMENT.

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

The guidelines reiterate the general compliance requirements under PDPA and provide action points concerning consent for collection, data breach notification, accountability and protection of children’s data. In addition, it also includes sample questions to consider when conducting a Data Protection Impact Assessment concerning children's data.

## OAIC INITIATES REVIEW OF NATIONAL HEALTH PRIVACY RULES 2021

The OAIC is planning to review the National Health Privacy Rules 2021 to ensure they remain fit for purposes. The 2021 rules which are set to be repealed on April 1, 2025 deal with the Australian government agencies that handle health information for the claim of health services. The OAIC is expecting submissions from interested stakeholders and the consultation form shall be available to the public from the second week of April 2024.

Australian Government
Office of the Australian Information Commissioner

# PRIVACY DIGEST

## PENALTIES, FINES AND TAKEAWAYS

### ICO ISSUES ENFORCEMENT NOTICE TO HOME OFFICE PILOT SCHEME FOR GPS MONITORING PRIVACY BREACH

The ICO issued an enforcement notice and warning to the Home Office pilot scheme for failing to assess the privacy intrusion of GPS monitoring on individuals arriving in the UK via unauthorized means. The Home Office violated Articles 35 and 5(2) of the UK GDPR by not adequately justifying the intrusive nature of continuous GPS tracking and failing to demonstrate why less invasive methods couldn't meet objectives. Additionally, their draft DPIA and guidance lacked effective data minimization demonstration. The Home Office must provide updated documents within 28 days, including revised data access forms, guidance, and a privacy notice covering past, current, and potential future data processing. They must also outline how the revised privacy notice will be provided to individuals with limited English proficiency.

### CJEU'S LANDMARK DECISION IN ENDEMOL SHINE CASE: ORAL DISCLOSURES AND PRIVACY RIGHTS

The CJEU, in the Endemol Shine case (C-740/22), addressed two key questions. Firstly, it affirmed that oral disclosure of personal information constitutes data processing under GDPR, interpreting the broad scope of "any operation" in Article 4(2). Secondly, regarding public access to court documents containing data on criminal convictions, the CJEU emphasized the need to balance this with fundamental privacy rights. It ruled that the seriousness of such data warrants prioritizing privacy over the public's interest in accessing official documents.

# 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.