Privacy Digest

AZURE DATA PROTECTION CONSULTANTS LLP

March 2024

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

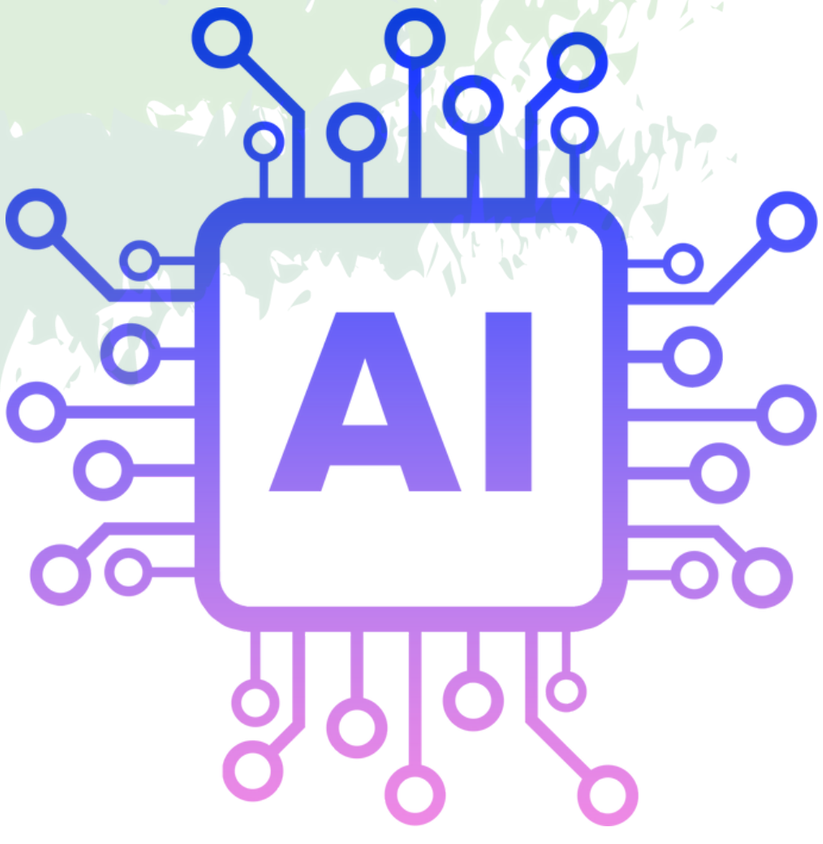
PRIVACY DIGEST

India is currently developing and putting into effect legislative frameworks to control many facets of artificial intelligence governance. Many initiatives and guidelines are in place to direct the responsible development and deployment of AI technologies in India, even if full rules specifically pertaining to AI are still in the process of being developed.

Latest Trends

National Artificial Intelligence Strategy

In 2018, India unveiled its first national AI policy, #AIFORALL, an inclusive approach to artificial intelligence. The plan emphasized the critical domains of healthcare, education, agriculture, smart cities, and transportation as areas of national importance for AI innovation and deployment. Since then, several of the strategy's recommendations—such as creating high-quality datasets to encourage research and innovation and putting in place legal frameworks for cybersecurity and data protection—have been successfully carried out.



PRIVACY DIGEST

DRAFT DIGITAL INDIA ACT

The draft Digital India Act 2023 is a proposed legislation in India aimed at replacing the existing Information Technology Act of 2000. The law, which was first introduced in June 2022, is anticipated to shortly be subject to public consultation. The Digital India Act addresses a wide range of topics, including cyber crime, data protection, online safety, and intermediary regulation, with the goal of creating a thorough legal framework for India's digital economy. It also calls for the establishment of a new government organization to supervise the digital sphere. We note that laws pertaining to artificial intelligence (AI) might establish certain “no-go areas” for businesses and online middlemen using AI and machine learning in applications that interact with end users.

MeitY
Government of India

DRAFT NATIONAL DATA GOVERNANCE FRAMEWORK POLICY

The draft National Data Governance Framework Policy (NDGFP) was made public by the Ministry of Electronics and Information Technology (MeitY) on May 26, 2022. This policy's main goal is to update and modernize government data gathering and management practices. According to the draft, the main goal of the NDGFP is to create a supportive environment for AI and data-driven research and start-ups in India through the creation of a sizable dataset repository. As the main components of the Framework call for the creation of the India Data Management Office under MeitY and the Digital India Corporation, the development of the India datasets platform, the establishment of request-based access to datasets, and the encouragement of private sector participation through the contribution of non-personal and anonymized data, India is taking steps to ensure best practices of transparency and inclusion.

PRIVACY DIGEST

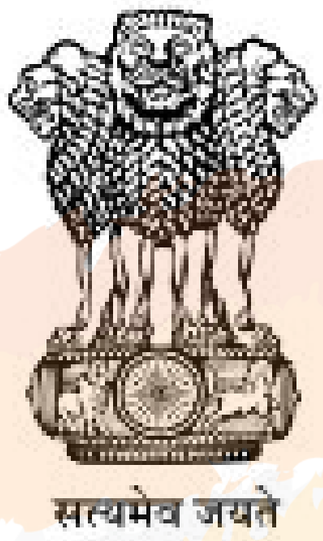
DRAFT INDIAN STANDARD: INFORMATION TECHNOLOGY – AI – GUIDANCE ON RISK MANAGEMENT

A committee within the Bureau of Indian Standards (BIS) is working on draft Indian Standards that are comparable to ISO Standards. As of right now, there are three draft Indian AI standards that are in line with international standards: ISO/IEC 24668, ISO/IEC TR 24372, and ISO/IEC 38507. The most recent draft, which is titled Guidance on Risk Management and is the same as ISO/IEC TR 24368, is currently available for public comment. By adopting an interoperable framework that complements the legal and regulatory framework, policies may be developed based on the technology architecture for artificial intelligence, which will expedite the deployment and usage of AI technologies.

GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE (GPAI)

Joining other renowned economies like the US, UK, EU, Australia, Canada, France, Germany, Italy, Japan, Mexico, New Zealand, South Korea, and Singapore, india has joined the Global Partnership on Artificial Intelligence (GPAI). With an emphasis on values like human rights, inclusion, diversity, creativity, and economic prosperity, the Global Partnership for Artificial Intelligence (GPAI) is an international project with a wide range of stakeholders that seeks to guide the responsible development and application of AI. The dates of the 2023 GPAI Summit are set for December 12–14, 2023, in New Delhi, India. AI specialists from a variety of industries are eligible to join GPAI working groups on an individual basis by self-nomination or through the recommendation of another GPAI member. They serve without representing their country or organization during their three-year term. At the moment, GPAI is inviting partners to engage in discussions regarding the challenges related to the trust of generative AI.

PRIVACY DIGEST



DRAFT REGULATORY FRAMEWORK OF AI

Rajeev Chandrasekhar, the minister of state for electronics and information technology, announced on Tuesday that the government will release a draft regulatory framework for artificial intelligence (AI) by June or July. Speaking at the first session of this two-day Nasscom leadership summit, he stated that the government is now developing a draft framework for AI regulations, which should be released in June or July of this year.

PRIVACY DIGEST

UK PRIVACY UPDATES

ICO APPROVED A NEW UK GDPR CERTIFICATION SCHEME AIMED AT ASSISTING LEGAL SERVICE PROVIDERS TO DEMONSTRATE COMPLIANCE WITH UK DATA PROTECTION LAWS.

The Legal Services Operational Privacy Certification Scheme (LOCS:23) is the fifth set of UK GDPR certifications that is intended to set out standards for technical and organizational requirements for legal service providers (both controller and processor) while processing personal data and maintaining client files.

To be certified under LOCS:2023, the applicant shall be required to document information related to client file processing activities in a manner prescribed along with the details of the technology used, third-party interactions and other processing activities during the lifecycle of the file.

ICO PUBLISHED A GUIDANCE ON CONTENT MODERATION.

The guidance defines content moderation as the analysis of user-generated content on user-to-user services to assess whether it meets certain standards.

Further, the guidance covers how UK data protection laws apply to content moderation and its impact on information rights. It is aimed at organizations who are carrying out content moderation under the scope of the Online Safety Act 2023 and at organizations who are carrying out content moderation for other reasons.

PRIVACY DIGEST

ICO PUBLISHED A NEW GUIDANCE NAMED “BIOMETRIC DATA GUIDANCE

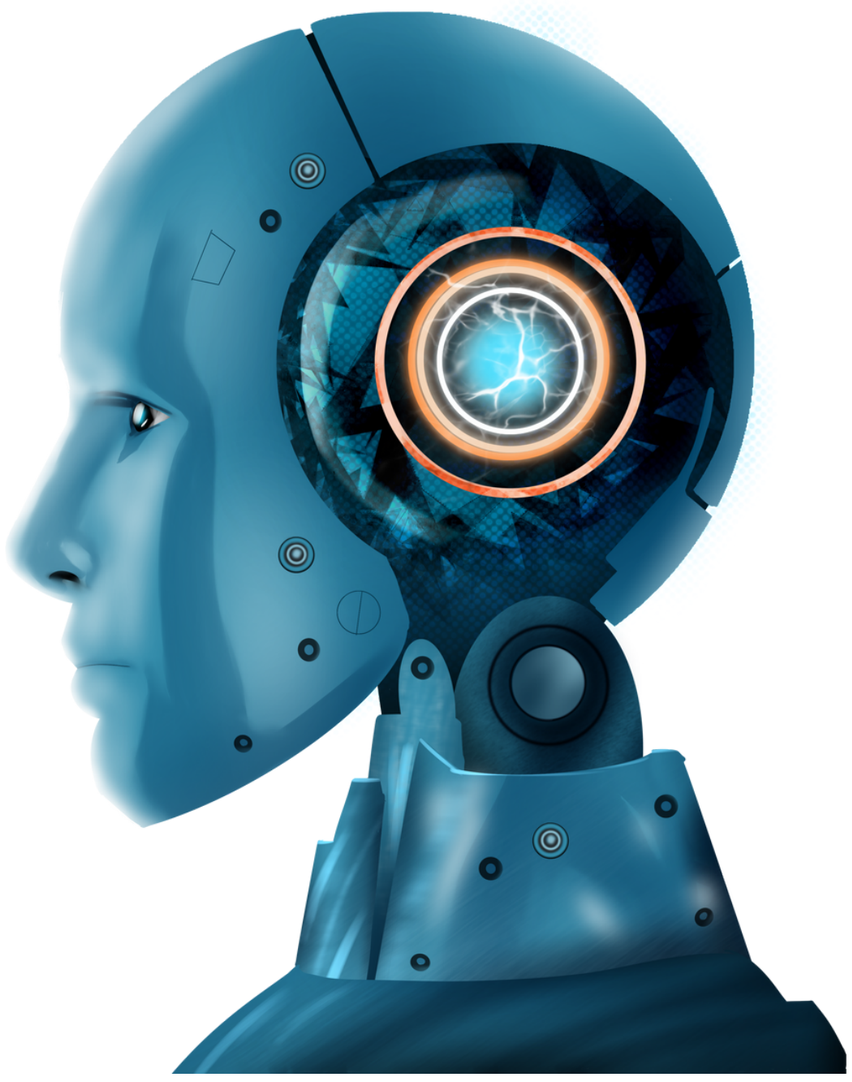
Biometric recognition” for organizations to comply with data protection laws while using biometric data to identify people.

This guidance is intended to highlight the considerations you should give to biometric data when you use biometric recognition systems. Therefore, it covers the definitions of biometric data under UK GDPR, biometric recognition uses and explains how these involve processing special category biometric data, and what organizations must, should and could do to comply with law and good practices for data protection compliance.

THE UK GOVERNMENT HAS RELEASED ITS RESPONSE TO PUBLIC FEEDBACK ON THE NATION'S AU REGULATORY STRATEGY.

The response reiterated the government's approach of being pro-innovative by combining cross-sectoral principles and context-specific framework, international collaboration and voluntary measures for developers to keep pace with uncertain advances in AI. Further, the government is.

- Planning to invest over 100 million pounds to realize new AI innovations and support the regulator's technical capabilities.
- Introduce a new steering committee with govt and regulator representatives to support coordination across the AI governance landscape.
- Reaffirming their stance mentioned in their AI regulation white paper published on March 2023.



PRIVACY DIGEST

THE UK INFORMATION COMMISSIONER'S OFFICE OPENED THE SECOND ROUND OF ITS GENERATIVE ARTIFICIAL INTELLIGENCE CONSULTATION.

The first round focuses on the lawful basis for web scraping to train generative AI models and this round focuses on how the principle of purpose limitation should be applied at different stages in the generative AI lifecycle. The Discussion recommended that the developers need to give careful consideration to purpose limitation before processing by:

• Setting out specific, explicit and clear purposes for each different stage of the lifecycle; and

• Explain what personal data is processed in each stage, and why it is needed to meet the stated purpose.

THE OFFICE OF DATA PROTECTION AUTHORITY ODPA, GUERNSEY HAD PUBLISHED A CONSENT GUIDANCE.

The guidance covers the essential basics for obtaining consent and provides a detailed checklist for:

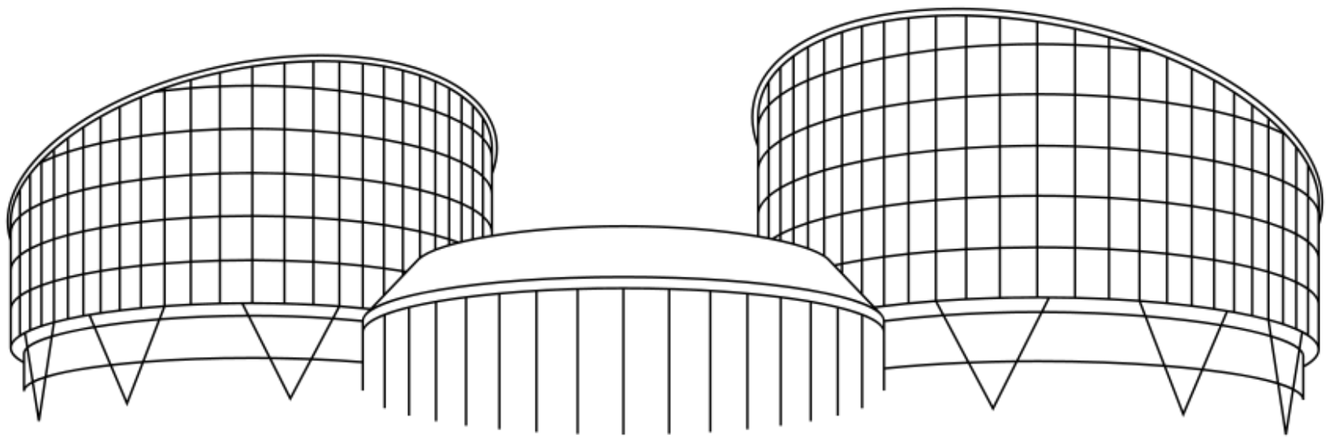
• Asking for consent
• Recording consent
• Managing consent

PRIVACY DIGEST

EU PRIVACY UPDATES

THE EDPB LAUNCHED A NEW, FREE AND OPEN-SOURCE WEBSITE AUDITING TOOL TO ASSIST ORGANIZATIONS WITH THEIR DATA PROTECTION COMPLIANCE.

The tool can be used by both legal and technical auditors, controllers, and processors and it is compatible with other tools such as the EDPS website evidence collector and assists in preparing and carrying out audits by a simple visit to the intended website.



EUROPEAN COURT OF HUMAN RIGHTS

COUR EUROPÉENNE DES DROITS DE L'HOMME

The European Court of Human Rights in the case of Pochasov v Russia, ordered that irrespective of the intention of the law enforcement agencies, introducing backdoors to weaken encryption could potentially enable widespread and indiscriminate surveillance of personal communication. Rather the court advocated for less intrusive methods for accessing communications that are currently available to law enforcement.

In this case, the Russian Federal Security Service under section 10.1 of Federal Law no. 149-FZ on Information, Information Technologies, and Protection of Information Act mandated Telegram to disclose all technical information, including the encryption key, to facilitate the decryption of communications for six users under the allegations of investigating terrorism-related activities.

MARCH 2024 — AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

The EU has launched a formal investigation on whether Byte Dance-owned video-sharing platform TikTok has breached online content rules under the Digital Service Act.

The investigation will focus primarily on the algorithmic design system of Tiktok which may stimulate behavioural addictions and whether Tiktok has put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors.

THE EUROPEAN AI OFFICE HAS BEEN FORMALLY ESTABLISHED BY THE EU COMMISSION.

The commission informed that the AI office will play a key role in implementing the AI act, enforcing rules for general-purpose AI models, collaborating with Member states and expert groups to exhibit well-informed decision making and promoting the EU's approach to trustworthy AI.

CJEU Advocate General issued an opinion in a case where without the consent of the data subjects, whether the General Data Protection Regulation (GDPR) allows a court enforcement officer to sell databases containing personal information in the context of enforcement proceedings. The Advocate opined that the operations carried out by the court enforcement officer to estimate the value of the databases concerned and sell them by public auction come within the scope of the GDPR and such processing constitutes a necessary and proportionate measure in a democratic society to achieve one of the objectives of general interest in GDPR.

PRIVACY DIGEST

EURACTIV

AS REPORTED BY EURACTIV, A LETTER SENT BY MEMBER OF THE EUROPEAN PARLIAMENT PAUL TANG,
raised serious questions regarding the potential impact of the UK's Data Protection and Digital Information Bill (DPDI) {which is intended to replace the UK GDPR} on the EU GDPR thereby weakening the protection of EU citizens.
Tang has raised three questions namely:

• Whether the commission consider the consequences that these provisions may have on law enforcement cooperation between the EU and the UK, for instance, within the Prüm I and Prüm II Framework or against the UK adequacy decision adopted under the Law Enforcement Directive?

• whether the Commission had evaluated the effects of the DPDI provisions on the protection of biometric data of European citizens under the GDPR and their compatibility with the European Court of Human Rights (ECtHR) ruling in S and Marper vs. UK?

• Does the Commission intend to annul the adequacy decision granting a free data flow between the EU and the UK once this bill is adopted?

PRIVACY DIGEST

COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

THE FRENCH DATA PROTECTION AUTHORITY (CNIL) HAS ISSUED GUIDANCE FOR THE COLLECTION OF DATA FOR MEASURING THE INDIVIDUAL PHYSICAL PERFORMANCE OF HIGH-LEVEL OR PROFESSIONAL ATHLETES.

CNIL observed that even if the measurement of individual physical sporting performance cannot be decorrelated from the study of the athlete's body, it essentially amounts to the collection and use of health data.
The guidance is divided into 5 key compliance requirements including:

• Has the role of data controller, joint data controller, and subcontractor been clearly defined?

• Are the fundamental principles of data protection (minimization, retention period, security measures, etc.) guaranteed?

• Is health data collected and stored? If so, has the possibility of invoking an important public interest to authorize this collection of health data been verified?

• Whether the purpose of the processing and the necessity or not of completing formalities been verified?

• If the above conditions are met, whether DPIA been carried out?

PRIVACY DIGEST

USA PRIVACY UPDATES

California Third District Court of Appeal overturned the decision of the Sacramento Superior Court ruling to stay enforcement of the CPRA regulation. Until March 29, 2024. The Appellate court indicates that CPRA does not require a year gap for enforcement and can be brought into force immediately.

NIST published a cyber security resource guide on how to comply with and implement the HIPAA security rule.

The resource consists of a compilation of key NIST publications, practical guidance and resources that are relevant to each HIPAA security rule standard to safeguard electronic protected health information (ePHI).

S. Sens. Ed Markey, D-Mass., and Bill Cassidy, R-La., announced a fresh group of bipartisan senators signed on to co-sponsor the proposed Children and Teens' Online Privacy Protection Act. The bill has been updated with small modifications based on the conversations with stakeholders and Senators Markey and Cassidy indicate that the newly updated COPPA 2.0 bill will create strong privacy protections for young people, ban targeted advertising to kids and teens, and create an Erase option for parents and kids by requiring companies to permit users to delete information.

MARCH 2024 — AZURE DATA PROTECTION CONSULTANTS LLP

PRIVACY DIGEST

U.S. SENATOR BILL CASSIDY, RELEASED A REPORT TO IMPROVE PRIVACY PROTECTIONS FOR AMERICANS' CRUCIAL HEALTH DATA.

The report outlines several proposals including how to consider data that cannot be clearly defined as health or non-health, how to consider protections for health data not covered by the HIPAA framework, such as information gathered through wearable devices and personal health applications, how to treat financial and geolocation data etc.

PRIVACY DIGEST

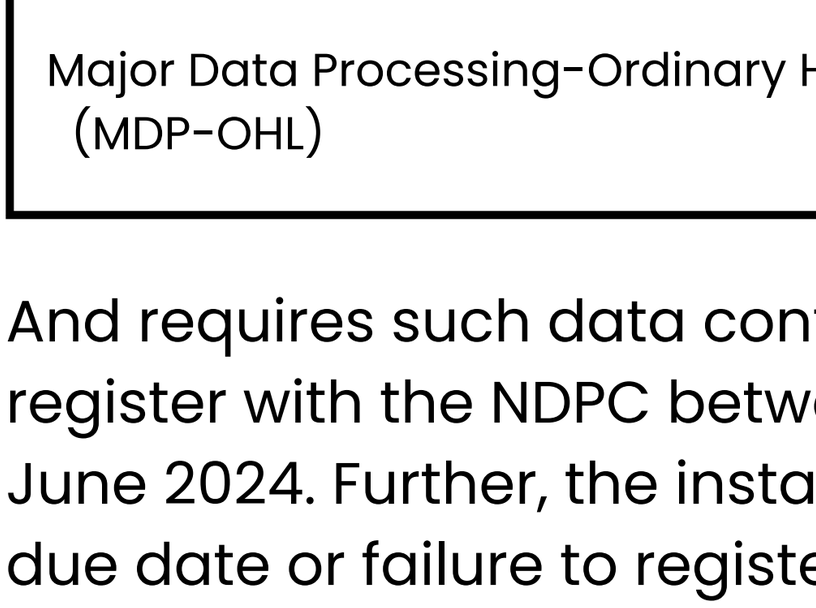
AFRICA PRIVACY UPDATES

Under section 44 of the Nigerian Data Protection Act (NDPA) which requires data processors and controllers of major importance to register with the commission within six months from the commencement of the act, the Nigerian Data Protection Commission has issued a guidance notice detailing the procedure and requirements for such registration.
The guidance notice classifies data controllers of major importance into three categories based on their level of processing namely:

Categories	Registration Fees (in Nigerian Naira)
Major Data Processing-Ultra High Level (MDP-UHL)	2,50,000
Major Data Processing-Extra High Level (MDP-EHL)	1,00,000
Major Data Processing-Ordinary High Level (MDP-OHL)	10,000

NDPC
NIGERIA DATA PROTECTION COMMISSION

And requires such data controllers and processors to register with the NDPC between 30 January 2024 and 30 June 2024. Further, the instances of Registration after the due date or failure to register shall be deemed as a default under the Act and shall be liable to a penalty as stipulated in the Act.



THE SOMALIA DATA PROTECTION AUTHORITY PUBLISHED GUIDANCE FOR THE IMPLEMENTATION OF THE DATA PROTECTION REGULATION (DPR) 2023.

The guidance comprises 4 step-by-step procedures to implement DPR, how to prepare an organization for DPR implementation, What the DPR audit requirements are to consider, what should be included in a DPR audit checklist etc.

PRIVACY DIGEST

SOUTH AMERICA PRIVACY UPDATES

THE NATIONAL DATA PROTECTION AUTHORITY PUBLISHED GUIDANCE ON LEGAL BASIS FOR DATA PROCESSING – LEGITIMATE INTEREST.

The guidance provides the interpretation and application of legal hypothesis of instances where legitimate interest can be deployed and further introduces a balancing model test comprising 3 phases namely: purpose, necessity and balancing safeguards. This guidance shall not apply to the processing of sensitive personal data.

The National Data Protection Authority (ANPD) prepared a "Personal Data Protection and Privacy Glossary" to systematize the main terms and expressions widely used in LGPD, as well as in documents and other communications published by ANPD.
The glossary is aimed to improve legal certainty, and transparency and will be open to comments and contributions on an ongoing basis to update it opportunely.

Lawmakers from Peru presented a law to establish a legal framework for AI use and regulation.

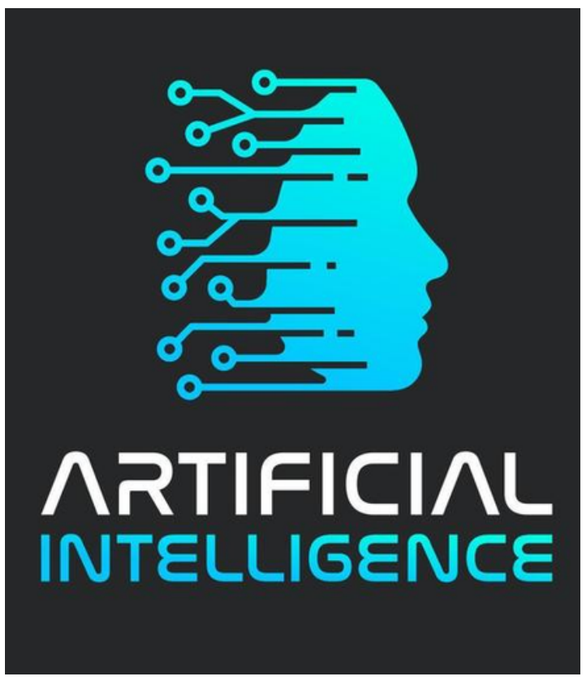
The law BoL 07033/2023 modelled on the EU AI Act consists of 30 sections and indicates a well-established risk classification, verification and certification and prohibitions and restrictions of AI practices. The act aimed to safeguard fundamental rights including privacy and ethical considerations in AI development and deployment.

PRIVACY DIGEST

The Argentina Agency of Access to Public Information and Federal Council for Transparency published "guidelines for the formulation of a personal data protection plan". The key highlight of the guideline includes a 15-headings guide for the development of a privacy policy and key information which shall be instituted under each of those headings.

PRIVACY DIGEST

ASIA PRIVACY UPDATES



ASEAN published a framework of AI governance and Ethics. The document serves as a guide for implementing national-level and regional-level recommendations that the governments can consider for implementing to design, develop and deploy AI systems responsibly in commercial and nonmilitary or dual-use applications. The guidance comprises 4 key components including**:**

• Internal governance structures and measures

• Determining the level of human involvement in AI-augmented decision-making

• Operations management

• Stakeholder interactions and communications.

The key guiding principles of this framework include Transparency and Explainability, Fairness and Equity, Security and Safety, Robustness and Reliability, Human-centricity, Privacy and Data Governance, Accountability and Integrity.

The Personal Information Protection Committee launched a 12-person committee named "Overseas Transfer Expert Committee" to evaluate whether the personal information protection level of national or international organizations is equivalent to Korea's level of personal information protection etc.

PRIVACY DIGEST

Personal Information Protection Commission

The Personal Information Protection Commission published guidance for providing pseudonymous information in the public sector.

The guide contains a four-step procedure to provide pseudonymous information and also highlights the physical, administrative and technical protection measures that be deployed for processing pseudonymous information. The guidance is only available in the Korean language.

PRIVACY DIGEST

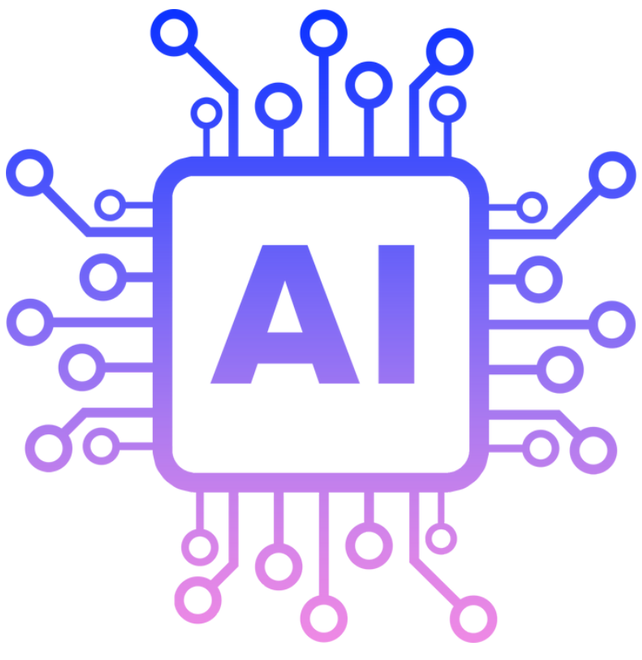
AUSTRALIA AND NZ PRIVACY UPDATES

Australian Government

Office of the Australian Information Commissioner

The office of the Australian Information Commissioner (OAIC) as a part of the periodical publication of Notifiable data breaches under the NBD scheme has published statistical information about data breaches from July 1 to Dec 31, 2023. The statistics highlighted that Malicious or criminal attacks remained the leading cause of data breaches i.e. 67% and human error preceded next with 30%. The top causes of human error include Personal information sent to the wrong recipient via email and unauthorized discourse or publication of Personal information.

Further, the OAIC commissioner highlighted that most of such breaches are accruing in cloud or software providers and highlighted the risk of outsourcing personal information handling to third parties.



According to the Australian Government's interim response to safe and responsible AI consultation, the Ministry of Industry and Science Ed Husic had announced the establishment of a 12-member new Artificial Intelligence Expert Group comprising of good mix of experts from law, ethics and technology.

The Group had already started their work and met for the first time on Feb 2, 2024, and will be in place until 30 June 2024. The group will provide advice to the Department of Industry, Science and Resources on immediate work on transparency, testing and accountability, including options for AI guardrails in high-risk settings, to help ensure AI systems are safe.

PRIVACY DIGEST

Privacy Commissioner
Te Mana Mātāpono Matatapu

The New Zealand Office of the Privacy Commissioner released a toolkit on how to create and evaluate privacy impact assessments.

The Privacy Impact Assessment toolkit contains information about the basic steps of a PIA, a template document of PIA to work with, a brief privacy analysis template to check whether it is necessary to do a full privacy impact assessment and a Risk and Mitigation Table template to identify, describe, and manage potential privacy risks involved.

Azure

Microsoft Azure has suffered a serious cyber-attack, thereby hundreds of mid-level and senior excavates' accounts have been compromised. The attack was first detected by Proof Point in late Nov 2023.

PRIVACY DIGEST

BREACHES, PENALTIES AND KEY TAKEAWAYS:

Information Commissioner's Office

The ICO has ordered public service provider Serco Leisure, Serco Jersey and seven associated community Leisure trusts to stop using FRTs and fingerprint scanning to record employee attendance.

ICO observed that the act of processing biometric data cannot be "necessary "when less intrusive means could be used to verify attendance. It also rejected the argument of Serco that biometric technology is the only way to prevent buddy punching and falsified time cards. The commission opined that there is no evidence provided by Serco to prove the abuse of other less intrusive means and it cannot rely on Article 6(1) (b) of UK GDPR to process biometric data, as this type of processing is not necessary to fulfil its employment contract.
Further, ICO rejected Serco's justification of using legitimate interest and it observed that in applying the balancing test to rely on legitimate interests, Serco has failed to give appropriate weight to the interest of data subjects considering the intrusive nature of biometric processing.

Finally, within 3 months, Serco has been ordered

• To cease all processing of biometric data for employment attendance checks from all Relevant Facilities and not implement biometric technology at any further facilities.

• Destroy all biometric data and all other personal and special category data that Serco is not legally obliged to obtain and retain.

PRIVACY DIGEST

DOORDASH

The California Attorney General has settled with DoorDash over allegations that the company violated the CCPA and CalOPPA by participating in marketing cooperatives and selling California customers' personal information without providing an opt-out notice. The AG found that DoorDash shared personal data, such as names and transaction histories, with cooperatives for targeted advertising without customer consent. The settlement requires DoorDash to provide opt-out methods for customers, disclose its participation in marketing cooperatives, and ensure compliance with CCPA and CalOPPA, including implementing do-not-sell forms and opt-out preferences.

The FTC fined Avast for unauthorized collection and sale of consumer browsing data.

The investigation found Avast collected and sold data to over 100 third parties without adequate disclosure. As part of the settlement, Avast must delete all collected browsing data, prohibit sale of such data for advertising, implement a privacy program, notify affected consumers, and obtain explicit consent before collecting or selling browsing data. The settlement also prohibits deceptive language in privacy policies and requires disclosure and opt-out options for tracking technologies.

PRIVACY DIGEST

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

The PDPC has imposed a financial penalty on Carousell, an e-commerce site for goods and property listings. The Penalty has been imposed as a result of two data breach incidents notified to the commission in 2022.
Background: the integrated chat function available for registered and unregistered users served them with all categories of property listings, due to human efforts, automatically exposed the email addresses and names of Guest Users to messages to listing owners of all categories in all markets. As a result, the personal data of 44,477 individuals comprising email addresses of all affected users and mobile phone 5 numbers of users in the Philippines were disclosed without their consent.

In another incident, after the Carousell has launched a public-facing Application Programming Interface ("API") during a system migration process. However, Carousell inadvertently omitted to apply a filter on that API, resulting in a vulnerability which was eventually exploited by a threat actor by scraping the accounts of 46 Subject Users with large numbers of associated Following/Follower Users, thereby obtaining the personal data of these Following/Follower Users.

Directions by PDPC:
• Review of software testing procedures.
• Avoid the practice of performing selective code reviews and tests.
• Review the processes and procedures for documenting functional and technical specifications of software.

Azure Data Protection Consultants LLP

Contact us for any queries:

https://azuredpc.com/

Azure Data Protection Consultants LLP

+91- 9599706305

support@azuredpc.com

DISCLAIMER