NEWSLETTER

AZURE DATA PROTECTION CONSULTANTS LLP

NOVEMBER 2022

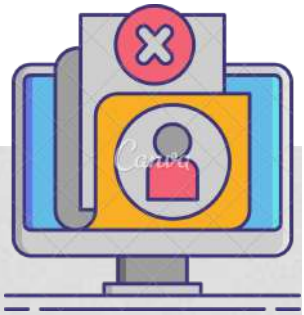
Your privacy digest is filled with the latest developments in the field of privacy and data protection across the globe.

News of the Year

DIGITAL PERSONAL DATA PROTECTION BILL

The Union Ministry of Electronics and Information Technology (MeitY) on 18th November 2022 published and sought inputs on the draft Digital Personal Data Protection Bill, 2022 (DPDP Bill), which seeks to replace the earlier Personal Data Protection Bill (PDP Bill) introduced back in 2019 and withdrawn in August 2022. While circulating the draft Bill, MeitY has invited comments from the public at large, which can be submitted by December 17, 2022.

The draft Bill covers processing (which includes collection /recording, storage, alteration, dissemination, removal/deletion, etc.) of personal data, the obligations of the data fiduciary, rights and duties of the data principal, and also sets up a compliance framework, which provides the establishment of a Data Protection Board.



Data Breaches

Thomson Reuters's 3TB of sensitive data leaked

November 1, 2022

Thomson Reuters left three of its servers accessible to anyone. The sensitive data contains sensitive information, up-to-date information including plain text passwords, and one data set containing access credentials to third-party servers. The accessible data was believed to be worth "millions" of dollars on the criminal forum and later on, the company recognized the issue and fixed it immediately.

Australian real estate group suffers data breach

November 3, 2022

Real estate group Harcourts self-reported a data breach in its Melbourne franchise. The database holds personal information relating to landlords, tenants, and trades and was used by the franchisee's service provider, Stafflink, to provide it with administrative support. The company will offer free credit monitoring and identity theft protection to impacted individuals. The Office of the Australian Information Commissioner was notified of the breach.



Royal Mail's customer data leaked *(November 3, 2022)*

The Royal Mail has suffered a data breach in its "Click & Drop" service which leaked customer data to other users. The company has explained that it has temporarily suspended the platform and that it is conducting an investigation into the issue. Customers could see the details of the parcel of the other customers. The U.K. Information Commissioner's Office said it had not yet been notified of the breach. ICO must receive notice within 72 hours of an organization identifying a breach.

Shangri La hotel group suffers data breach *(November 9, 2022)*

A data breach affected eight Shangri-La hotels in Singapore, Taipei, Tokyo, Hong Kong, and Chiang Mai, including a Singapore hotel where foreign government delegates attended a defense summit in June. The hotel group unveils it has received an email from hackers claiming responsibility for the attack. The hotel chain said it is unlikely the delegates were impacted by the breach. Hong Kong's Office of the Privacy Commissioner for Personal Data said personal data of more than 290,000 Hong Kong customers may have been compromised.

Medibank data leaked on dark web *(November 9, 2022)*

Data of Medibank customers was posted on a blog linked to the Russian ransomware group REvil, including names, addresses, birthdates, and Medicare numbers. Medibank has said 9.7 million current and former customers are affected by the breach. That includes 5.1 million Medibank customers, 2.8 million ahm customers, and 1.8 million international customers. Health claims for about 160,000 Medibank customers, 300,000 ahm customers, and 20,000 international customers were accessed. The information exposed includes service provider names and codes associated with diagnosis and procedures.

Manitoba hospital workers violated patient privacy *(November 10, 2022)*

Manitoba hospital workers were found to violate patients' privacy more than 1,000 times in the last 3 years. Hospital workers in the province breached patient data more than 1,100 times from January 2019 through April 2022, and questions remain if workers were disciplined for the violations. Hospital human resources officials either said disclosing the nature of employee discipline would violate their right to privacy or such records were not kept out of concern for potential privacy violations.

US Medical processors suffer breach *(November 16, 2022)*

A server misconfiguration at a firm that provides medical claims processing for correctional facilities exposed sensitive information of nearly 600,000 inmates who received medical care during the last decade which included PII. CorrectCare Integrated Health reported at least three "unauthorized access/disclosure" & breaches to the U.S. Department of Health and Human Services.

Russian scooter-sharing service suffers data breach *(November 17, 2022)*

Russian scooter-sharing service Whoosh reported a hack of its database containing personal data belonging to 7.2 million people. Whoosh operates in 40 Russian cities, offering more than 75,000 scooters for residents' urban transportation needs. A hacker reportedly began selling stolen data in an online forum in the form of promotional codes for free services, which included customer identification and payment information.

Grocery Chain in Canada suffers data breach *(November 18, 2022)*

Canadian grocery chain Sobeys suffered a data breach which was announced by the Office of the Information and Privacy Commissioner of Alberta and the Commission d'accès à l'information du Québec. The reports of customers suffering difficulties in the filing process and the company also suffered IT system issues from the customers. The Office of the Privacy Commissioner of Canada is also in communication with the company.

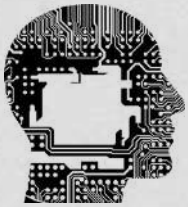
New Appointments / New laws

Framework for facial recognition agreed by national data regulators *(November 1, 2022)*

At the 44th Global Privacy Assembly in Istanbul, Turkey, data protection regulators from more than 120 countries agreed to a framework for using personal data with facial recognition. The facial recognition resolution is based on six core principles, which must be deployed with a "clear legal basis." The entity employing the technology must establish "its reasonableness, necessity, and proportionality," and human rights assessments must be conducted so the use of the technology is transparent to the surveilled persons.

EU Digital Markets Act comes into *effect (November 1, 2022)*

EU DMA (Digital Markets Act) has entered into force. The new regulation will end the unfair practices by companies that act as gatekeepers in the online platform economy. The DMA defines qualifying large online platforms as "gatekeepers" and establishes a list of "do's and don'ts" they must implement "to ensure fair and open digital markets." The provisions will be applied starting 2 May, 2023.



Data Protection Law draft submitted in Ukraine
(November 2, 2022)

A data protection draft law has been submitted to Ukraine's parliament. The draft proposes to regulate the processing of personal data and other types of data which includes biometric information. The current legislation does not ensure the protection of the data.

Pennsylvania Bill to create Artificial Intelligence Registry
(***November 3, 2022)***

Members of the Pennsylvania House of Representatives introduced a bill to create a state Artificial Intelligence Registry. The Bill provides for establishment of a registry of businesses operating AI systems within the state. The registry would feature information such as the business name, IP address, type of code the business is using AI for and the software's intent. As per the bill draft, the Department of State would be prohibited from selling data contained in the registry for commercial purposes.

EU Digital Services Act comes into force *(November 16, 2022)*

The European Union Digital Services Act comes into force, which provides for new obligations for online platforms to reduce harm online and introduce stronger user protections. The DSA applies to all digital services that connect consumers to goods, services, or content. Covered entities will have four months to comply with obligations under the DSA.

German DPA releases processor Code of Conduct
(November 18, 2022)

A Code of Conduct for processors has been released by the Baden-Württemberg State Commissioner for Data Protection and Freedom of Information. The Code of Conduct offers standardized rules to support companies in applying the EU General Data Protection Regulation. Processors following the code submit to regular monitoring by a body accredited by the LfDI.

ICO published Transfer Risk Assessment Guidance
(November 21, 2022)

UK ICO published and announced the new guidance and resources for data transfer risk assessments. The ICO said its guidance presents an alternative, achievable approach compared to the European Data Protection Board& guidelines and touted the assessment process as reasonable and proportionate. The assessment tool rolled out by the ICO evaluates risk based on whether the transfer significantly increases the risk of either privacy or other human rights breach.

Cyber Resilience Act draft released by EU council
(November 23, 2022)

The Czech Presidency of the Council of the European Union released the new text on the proposed Cyber Resilience Act, is legislation intended to enact cybersecurity requirements for connected devices and related services. The member states are not prevented from imposing national restrictions on digital products, including bans, based on national security.

UK and South Korea agree on an Adequacy Decision ***(November 23, 2022)***

Since departing the EU, the UK has agreed to its first adequacy decision with South Korea which was announced by The U.K. Department for Digital, Culture, Media, and Sport. The DCMS said the decision and its new freedoms will benefit many small and medium-sized businesses that may have avoided international data transfers to Korea due to these burdens. The decision and subsequent legislation were presented to U.K. Parliament and are expected to take force on Dec. 19.

ICO and Ofcom share online safety data protection regulatory goals ***(November 25, 2022)***

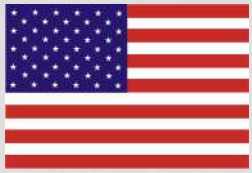
The U.K. Information Commissioner Office and communications regulator Ofcom released a joint statement on shared regulatory goals around online safety and data protection. The regulators will work closely to ensure policies are consistent and establish clear expectations for organizations to meet both online safety and data protection requirements.

PIA guide published by Israel's PPA *(November 23, 2022)*

Israel's Privacy Protection Authority published a guide with detailed recommendations on conducting privacy impact assessments (PIA). The PPA said the guide assists organizations in identifying privacy risks at an early stage and will help them deal with them in a simpler and more efficient way, and usually, also at a lower financial cost. While privacy impact assessments are not mandated by Israeli law, the PPA said reviewing privacy impacts when setting up and managing new projects benefits the organization and its customers.

Council of the EU approves NIS2 Directive *(November 28, 2022)*

The Czech Presidency of the Council of the European Union approved the NIS2 Directive, a modernized framework based on the EU Network and Information Security Directive. The directive will soon be published in the Official Journal of the European Union and take effect 20 days thereafter. Member states will have 21 months to incorporate the directive into national law.



EDPS and ENISA agree to data security cooperation ***(November 30, 2022)***

The European Data Protection Supervisor and the European Union Agency for Cybersecurity signed a memorandum of understanding to forge strategic cooperation on data protection and cybersecurity matters. The entities described the MOU as a partnership for designing, developing, and delivering awareness campaigns and joint work on cybersecurity aspects of data protection. The agreement also includes commitments to adopting privacy-enhancing technologies and increasing the relevant capacities and skills of EU public-sector personnel.

Hamburg authority published advisory on EU-US Data Privacy Framework ***(November 30, 2022)***

Hamburg DPA published its advisory and observations on EU-US Data Privacy Framework. The HmbBfDI advised data transfer impact assessments must follow the ruling by the Court of Justice of the European Union on lawful EU-U.S. transfers until the proposed DPF is finalized. The regulator also said the U.S. executive order to stand up the DPF 'deserves a well-founded, open-ended examination' and 'actual application' of provisions for proportionality, and the Data Protection Review Court will be closely monitored.

Australia passes Privacy Legislation Amendment Bill 2022 ***(November 29, 2022)***

The Parliament of Australia approved the final passage of the Privacy Legislation Amendment Bill 2022. The bill amends the Privacy Act of 1988 to increase data breach fines to AU$50 million, or penalties based on data monetization and 30% of adjusted quarterly turnover under a new three-factor penalty scheme. The bill facilitates consumer remedies as well as helps the regulators efficiently.

Tanzania parliament passes the Personal Data Protection Bill ***(November 8, 2022)***

Tanzania's Parliament passed the Personal Data Protection Bill 2022. The bill establishes a Commission for the Protection of Personal Data, which would have the authority to issue fines for the mishandling of personal data and set policies and procedures for the handling of such data.

Fines and Settlements

SolarWinds agree to 26M$ settlement over data breach *(November 3, 2022)*

SolarWinds has agreed tentatively 26M$ fine with US SEC to settle a lawsuit over its cybersecurity disclosures ahead of a December 2020 breach that exposed the data of thousands of companies and government offices. SEC alleged that the company violated U.S. securities law with respect to its cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures.

Google reached a settlement over location tracking with 40 states *(November 14, 2022)*

Google reached a $391.5 million settlement with 40 state attorneys general over allegations its location tracking misled users. The state attorneys general said the settlement, which followed a four- year investigation, is the largest involving internet privacy by U.S. states. Under the settlement, Google agreed to clarify its location tracking disclosures in 2023.

CNIL fines 800k euros to Discord for GDPR violations
(November 17, 2022)

CNIL fined software developer Discord 800,000 euros for failing to comply with EU General Data Protection Regulation requirements on data retention periods and personal data security. The CNIL said it took into account Discord's efforts to reach compliance throughout its investigation when deciding the amount of the fine.

Perfume chain company fined 1.4M euros by Garante
(*November 30, 2022)*

Garante, Italy's data protection authority fined perfume chain Douglas Italia 1.4 million euros for data protection violations. The company retained data of more than 3 million customers without requesting consent for processing. In addition, the company is required to adopt compliance measures regarding data retention times and data processing for marketing and profiling purposes, and must delete data from the past 10 years.

Meta fined 265M euros for failure to prevent Data Scrapping by Irish DPC
(November 29, 2022)

Ireland's Data Protection Commission announced a 265 million euro fine to Meta over alleged EU General Data Protection Regulation violations. The fine is the third-largest GDPR penalty served to date. The probe concluded the platform violated Articles 25(1) and 25(2) of the GDPR. The decision also requires Meta to bring its processing into compliance by taking a range of specified remedial actions within a particular timeframe.

Azure Data Protection Consultants LLP

Contact us for any queries:

http://www.azuredpc.com

Azure Data Protection Consultants LLP

+91- 9599706305

DISCLAIMER