PRIVACY DIGEST

Ministry of Electronics and Information Technology
Government of India

MEITY PULLS DOWN DRAFT DATA ANONYMISATION GUIDELINES

SEPTEMBER 8, 2022

The government has pulled down its draft guidelines on data anonymisation which is the third such instance of a public consultation being removed this year. The guidelines were put up for feedback by the Ministry of Electronics and Information Technology (MeitY) on August 30. The draft states that all e-governance projects apply data anonymisation as a norm and identify and record exceptions. After hosting it on its egovstandards website, MeitY has removed it completely.

INDIA PROPOSES A DRAFT OF THE TELECOMMUNICATION BILL

SEPTEMBER 23,2022

The Indian Parliament published the draft Indian Telecommunication Bill 2022, which aims to regulate digital communications. The 40-page draft proposes to grant the government the ability to intercept messages beaming through internet-powered communication services in the case of any public emergency or the interest of public safety while providing the government immunity against any lawsuit. The legislation, for which the ministry will seek public comments until October 20, additionally attempts to take broader steps to curb spam messages by proposing consent requirements and a "Do Not Disturb" registry.

NEW APPOINTMENTS / NEW LAWS

INDIA MIGHT NOT FOLLOW EUROPE ON DATA PROTECTION

SEPTEMBER 26, 2022

In an interview with The Indian Express, Indian Minister of State for Electronics and Information Technology, Rajeev Chandrasekhar talked about the potential features of the country's reworked data protection bill. He stated that India would not be following Europe on data protection adding that India's next draft data protection bill will have to "figure out whether the weightage is on adequacy, privacy, or ease of doing business."

DELHI HC ISSUES NOTICE ON CHALLENGE TO CERT-IN DIRECTIONS (SNT HOSTINGS V. UNION OF INDIA)

SEPTEMBER 29, 2022

Delhi high court has agreed to hear a challenge to the Indian Computer Emergency Response Team's April directives where it required virtual private network (VPN) service providers to store names, email IDs, contact numbers, and IP addresses of customers for a period of five years. The petitioner has challenged CERT-In's directives, arguing that it went beyond CERT-In's authority by asking service providers to store personal and invasive information about customers. The high court has given CERT-In four weeks to respond to the challenge. The case will be heard again in court on Dec. 9.

DATA PROTECTION BILL LIKELY TO BE INTRODUCED IN THE PARLIAMENT

SEPTEMBER 29, 2022

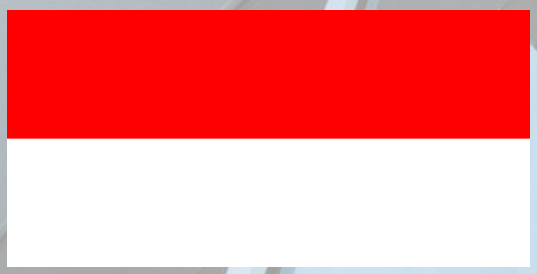
Solicitor General Tushar Mehta on behalf of the Central Government has told the Supreme Court that a new Bill will be introduced in Parliament regarding Data Protection. So, the 5 judge bench has asked the government that either the Bill should be placed early or it will begin the final hearing of the WhatsApp-Facebook Privacy case (Karmanya Singh Sareen v. Union of India) on January 17, 2023, while the pleading in all the cases is to be completed by December 15, 2022.

NEW APPOINTMENTS / NEW LAWS

GERMANY'S BSI PUBLISHES THE SECOND EDITION OF ITS REPORT ON CYBERSECURITY IN THE AUTOMOTIVE SECTOR

SEPTEMBER 19, 2022

According to the report, the future of cars will rely more on IT systems, for instance, the control of the vehicle and the car's networking infrastructure. The BSI said new technologies in vehicles could not be susceptible to a cyberattack that could compromise driving safety.



INDONESIA'S NEW DATA PROTECTION BILL

SEPTEMBER 20, 2022

Indonesia's parliament passed a long-awaited data protection bill on September 20. The bill also authorizes the president to create an oversight body to enforce the law. The law includes the potential confiscation of assets, fines of up to 2% of a company's annual revenue, and a stipulation that individuals could be imprisoned for up to six years for falsifying personal data or up to five years for collecting personal data illegally.

ATTEMPT TO ELIMINATE ANTI-DRUNK DRIVING TECHNOLOGY TO PREVENT PRIVACY VIOLATIONS

SEPTEMBER 1, 2022

Three U.S. Senators are attempting to eliminate a drunk and impaired driving prevention technology provision from the Infrastructure Investment and Jobs Act. The provision in the infrastructure bill gives regulators a minimum of three years to develop drunk driving-detecting tech and gives automakers two years to implement the tech into their vehicles. U.S. Sens. Mike Rounds, R-S.D., John Cornyn, R-Texas, and Mike Braun, R-Ind., co-sponsored the Safeguarding Privacy in Your Car Act, which would limit the use of such tech due to the potential for privacy violations.

NEW APPOINTMENTS / NEW LAWS

DEMOCRATS CALL ON HHS TO PROTECT ABORTION RIGHTS AND PRIVACY UNDER HIPAA

SEPTEMBER 14, 2022

Thirty Democratic senators called on the Department of Health and Human Services (HHS) to take immediate action to safeguard women's privacy and their ability to safely and confidentially get the health care they need. In a letter to HHS Secretary Xavier Becerra, the Senators urged the Biden Administration to strengthen federal privacy protections under the Health Information Portability and Accountability Act (HIPAA) to broadly restrict providers from sharing patients' reproductive health information without their explicit consent—particularly with law enforcement or in legal proceedings over accessing abortion care.

CALIFORNIA FIRST WITH LAW PROTECTING CHILDREN'S ONLINE PRIVACY

SEPTEMBER 15, 2022

Governor Newsom signed Assembly Bill 2273, establishing the California Age-Appropriate Design Code Act. CAADCA, AB 2273 requires businesses with an online presence to complete a Data Protection Impact Assessment before offering new online services, products, or features likely to be accessed by children. The Children's Data Protection Working Group will be established as part of the California Age-Appropriate Design Code Act to deliver a report to the Legislature, by July 1, 2024, on the best practices for implementation.

LAWSUIT FILED AGAINST META FOR ALLEGEDLY BYPASSING APPLE PRIVACY SETTINGS

SEPTEMBER 23, 2022

Two class action suits have been filed against Meta on behalf of apple iOS users for allegedly bypassing privacy preferences. Google alleged that Meta sought to recoup lost advertising revenue by inserting a tracking code on external websites their user visited while using the in-application browser for Facebook or Instagram.

NEW APPOINTMENTS / NEW LAWS

CANADIAN PARLIAMENT RESPONDS TO COMMITTEE REPORT ON MOBILITY

SEPTEMBER 23, 2022

Member of parliament submitted a response to the House of Commons committee on access to Information, Privacy and Ethics' report on Public Health Agency of Canada's collection and use of mobility data during the COVID-19 pandemic. Mona Fortier responded to the committee's 22 recommendations for updated data practices, addressing the suggestions based on theme grouping specific to mobility data, general data and legislative reform.

US APPELLATE COURT DECISION PAVES WAY FOR MULTIPLE TRACKING LAWSUITS

SEPTEMBER 26,2022

A recent US appellate court decision against advertising technology company for an alleged Pennsylvania law violation has led to other lawsuits against online companies. NaviSton violated a Pennsylvania wiretapping law when it and retailer allegedly used tracking tech that sends an e-mail to anonymous web users after the complainant visited a website.

NEW APPOINTMENTS / NEW LAWS

INSTAGRAM WAS FINED €405M FOR VIOLATING KIDS' PRIVACY BY THE IRISH DPC

SEPTEMBER 6, 2022

The Irish Data Protection Commission has fined Meta-owned social media platform Instagram €405 million for children's privacy violations under the GDPR. The penalty, currently the highest for a Meta-owned company, is aimed at Instagram's violation of children's privacy, including its publication of kids' email addresses and phone numbers. The Irish DPC has at least six other investigations into Meta-owned companies in the pipeline. A Meta spokesperson said that "the inquiry focused on the old settings that we updated over a year ago" and it is "carefully reviewing their final decision."

AIRLINE SUFFERS A DATA BREACH

SEPTEMBER 20, 2022

American Airlines notified customers the company experienced a data breach over the summer. American Airlines discovered the breach on July 5 and immediately secured the impacted email accounts and hired a cybersecurity forensic firm to investigate the security incident. The company determined employees' and customers' personally identifiable information could have been exposed. In response, American Airlines will offer impacted customers two years of free credit monitoring. The company is yet to disclose the number of affected customers and how many email accounts were breached in the incident.

DATA BREACHES

MORGAN STANLEY FINED $35M BY US SEC OVER ALLEGED DATA PROTECTION, DELETION ISSUES

SEPTEMBER 20, 2022

The U.S. Securities and Exchange Commission (SEC) announced a $35 million settlement with multinational financial services provider Morgan Stanley Smith and Barney's wealth and asset management division related to alleged insufficient data protection measures for approximately 15 million customers over a five-year period. It was alleged that there were various data deletion issues, including those occurring via a contracted third-party moving and storage company that had no appropriate expertise or measures for data destruction services.

BERLIN DPA IMPOSES 525K EURO FINE OVER DPA VIOLATION

SEPTEMBER 22, 2022

Berlin commissioner for data protection and freedom of information issued a 525K euro fine to a Berlin based retailer for violation of EU GDPR. An investigation found an alleged conflict of interest concerning the DPO's employment status and decision making responsibilities that violated article 38(6) of the GDPR.

AUSTRALIAN TELECOMMUNICATIONS PROVIDER SUFFERS CYBERATTACK

SEPTEMBER 22, 2022

Australia's second-largest telecommunications company, Optus, has reported a cyberattack. The breach exposed personally identifiable information such as customers' names, dates of birth, phone numbers, and email addresses. However, Optus says payment data and account passwords were not compromised. The company announced it would notify those at "heightened risk" but all customers should check their accounts.

DATA BREACHES