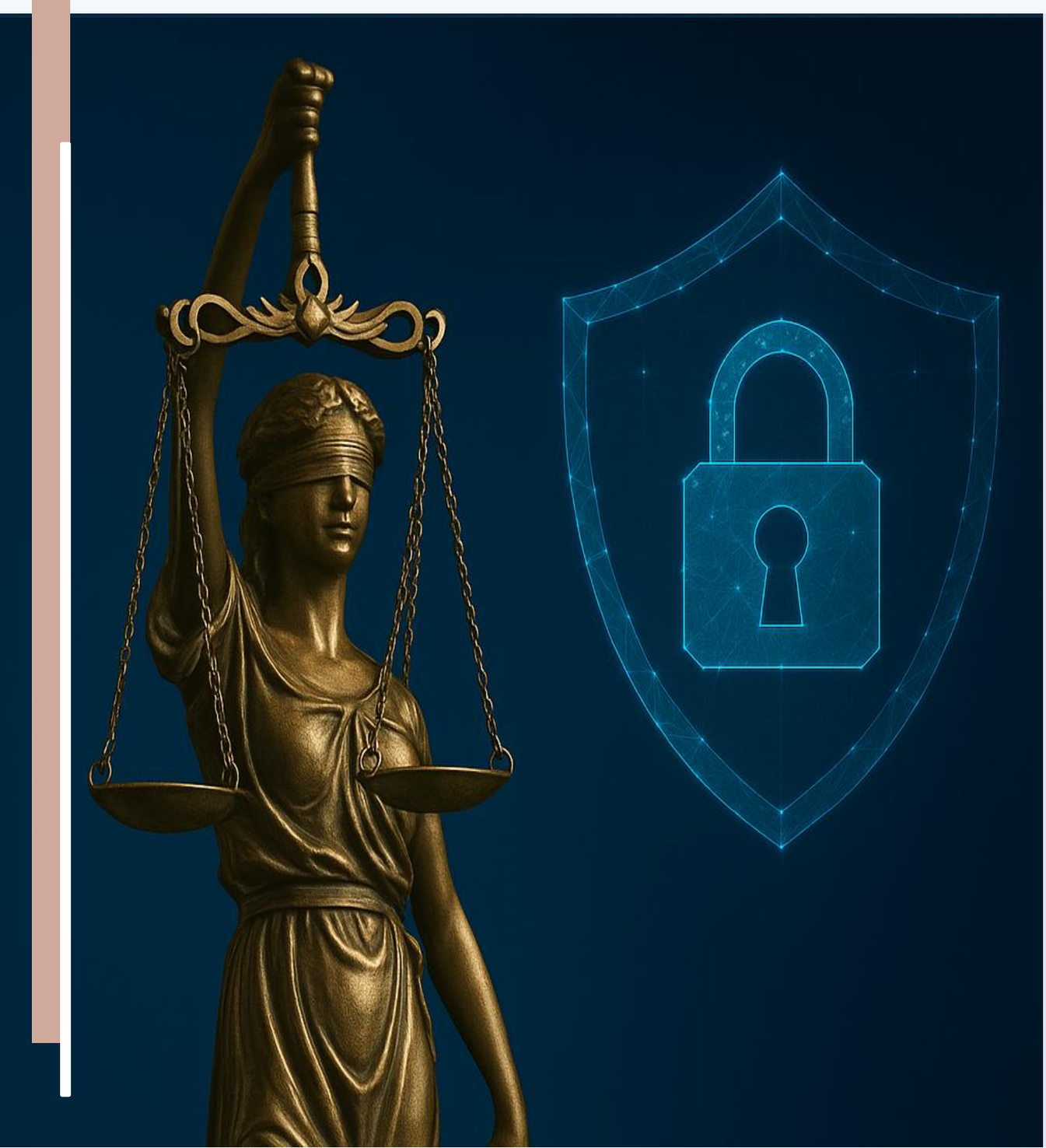
SHIVADASS & SHIVADASS®
LAW CHAMBERS

COMPETITION, DATA PROTECTION & PRIVACY SNIPPETS

1st Ed.



Quarterly Update June 2025

NEWS ALERTS

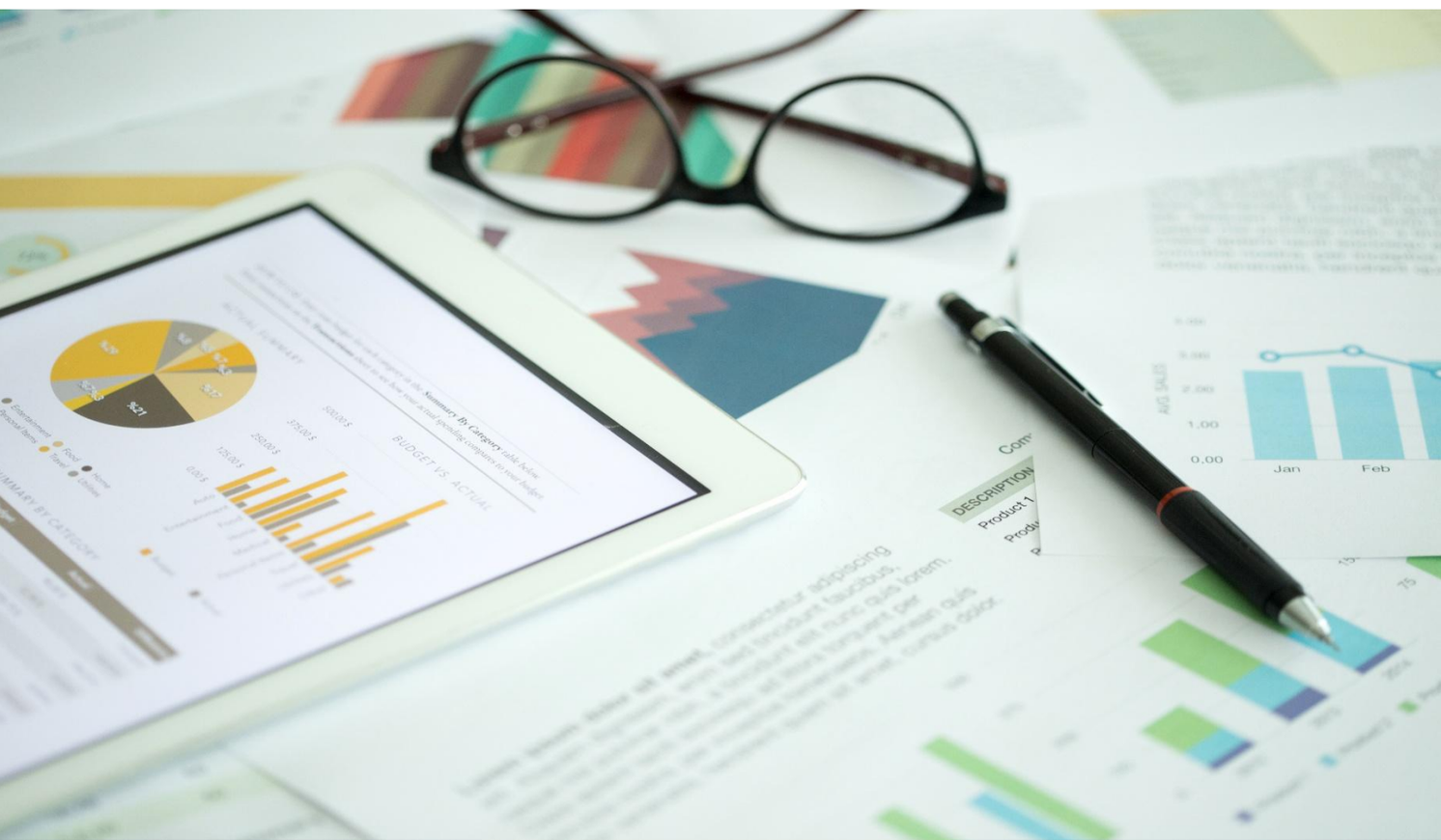
CCI accepted Google's settlement offer in the Android TV case. The final settlement amount is INR 20.24 crores. ***(Case No. 19 of 2020)***

NCLAT refuses to stay CCI's sanctions on UFO Moviez India Pvt. Ltd. and Qube Cinema Technologies Pvt. Ltd. for tie-in arrangements, exclusive supply agreement and refusal to deal that contravened Section 3(4) of the Act and hindered competition in the digital cinema exhibition and post-production processing markets. ***(Competition Appeal (AT) No.8 of 2025)***

CCI closes abuse of dominance proceedings against Hindalco Industries Ltd. and Vedanta Ltd. after failing to find a *prima facie* case. The information had alleged that the Hindalco and Vedanta abused their dominant position by imposing unfair and discriminatory conditions in their Marketing Policy on purchase of goods. ***(Case No. 31 of 2024)***

CCI closes Section 3 and 4 proceedings against Canara Bank. The information alleged *inter alia* that the bank had arbitrarily raised interest rates, prevented the informant from transferring loans to other banks, initiated SARFAESI proceedings, and entered into anti-competitive agreements with valuers. The CCI found that the bank did not have dominance in the market, and that there was no arbitrary raise in interest rates or existence of any anti-competitive agreements. ***(Case No. 35 of 2024)***

NCLAT stayed CCI's order preventing WhatsApp from sharing user data collected on its application with other Meta companies for advertising. It is to be noted that the CCI's direction to WhatsApp to enhance transparency and implement user choice in sharing their data with other Meta companies for purposes other than advertising. The monetary penalty of INR 213 crores is stayed subject to WhatsApp depositing 50% of the penalty amount. ***(Competition Appeal (AT) No. 1&2 of 2025)***



LANDMARK CASES

Volume-based discounts are not per se anticompetitive

- The Supreme Court recently held that slab discounts were provided to all purchasers, and Schott Glass' JV was able to reach the top slab due to its capacity to purchase larger quantities.
- There was no condition placed by Schott Glass to restrict buyers from approaching other vendors. While the JV enjoyed a monthly credit cycle which was not offered to other entities, the same was based on valid reasons and could not be a basis to establish violation of competition law, especially when the JV was not offered different rates.
- The Court further observed that the long-term agreement with JV does not cause a foreclosure of the downstream market as Schott Glass did not participate in the downstream market, and there was no evidence to show shrinking in the number of competitors.
- Further, the Supreme Court found that the CCI's original order and DG's investigation were invalid due to the denial of Schott Glass's right to cross-examine witnesses who had alleged that SGIPL had engaged in forced bundling.
- The Court referred to Section 36 of the Competition Act, 2002, and Regulation 41(5) of the CCI General Regulations, which obliges the CCI/DG to grant opportunities for cross-examination. However, the Regulation grants discretion to the CCI or the Director General to refuse cross-examination if the same is not necessary or expedient.

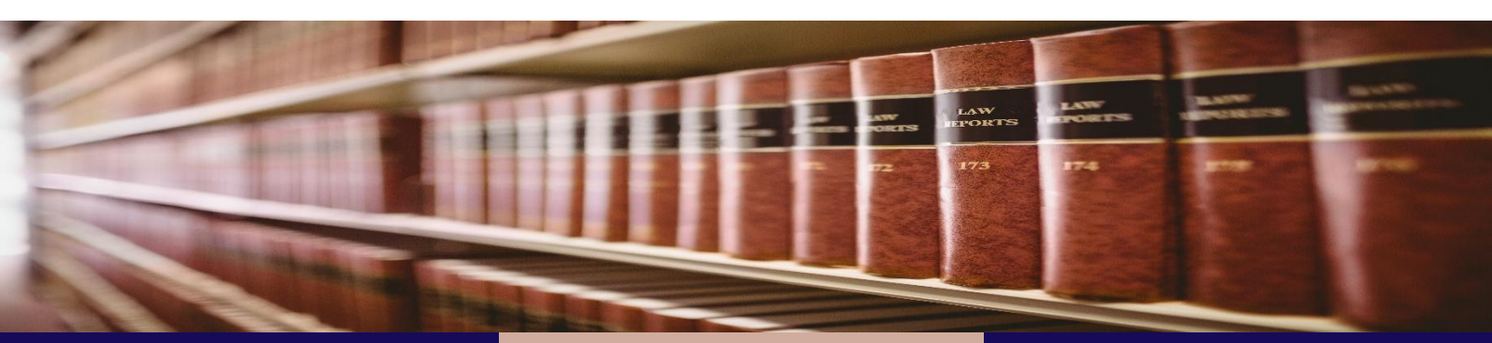
Competition Commission of India v. Schott Glass India Pvt. Ltd., C.A. No. 5843/2014

Interplay between competition and IBC timelines

- The Supreme Court held that the term "prior" in the proviso to Section 31(4) of the IBC must be construed in its plain meaning and rejected purposive interpretation offered by AGI.
- The Supreme Court set aside the CoC's approval of AGI's plan and restored all stakeholders to *status quo ante* positions. It directed the CoC to re-consider all resolution plans that had secured CCI approval by that date.
- An observation was made by the Supreme Court that the procedure under Section 29 of the Competition Act must be mandatorily followed by the CCI in investigating every proposed combination.
- In May 2025, the Court **allowed CCI's review petition,** clarifying that **Section 29(1A)** of the Competition Act, which deals with Director General-led investigations after a prima facie finding of AAEC, is **discretionary and not mandatory**. The Court emphasized that once an SCN is issued under Section 29(1), the CCI is not bound to escalate every case to a DG investigation.

AGI Greenpac Ltd. v. Independent Sugar Corporation Ltd., C.A. No. 6071/2023;

Competition Commission of India v. Independent Sugar Corporation Ltd., R.P. (C) No. 482/2025 in C.A. No. 4924/2023



REGULATORY

2025 Predatory Pricing Regulations

- The CCI notified the Determination of Cost of Production Regulations, 2025 while repealing the 2009 Regulations.
- The revised regulations are aligned with contemporary economic theory, and judicial interpretation concerning the evaluation of predatory pricing under Section 4(2)(a)(ii) of the Act.
- Key definitions such as “total cost” now explicitly include depreciation while excluding financing overheads to achieve consistency in cost assessment.
- The definitions of “total variable cost” and “average avoidable cost” have been tweaked for ease of interpretation and application.
- A significant change has been made with respect to the revised definition of “long run average incremental cost” (LRAIC), which shall now include all fixed, variable, and sunk costs directly or indirectly attributable to production, including common costs in multi-product firms.
- Market value has been omitted from the regulations as it includes values that are not dependent purely on cost and are influenced by market conditions.
- It is also clarified that experts may be engaged solely to *assist* the Commission in cost determination, with final authority resting with the Commission.
- The new regulations continue to be sector-agnostic and continue to provide flexibility to the CCI to tackle emerging industries like digital markets. The regulations only prescribe procedural framework and do not affect the substantive jurisprudence on predation.

Competition Commission of India (Determination of Cost of Production) Regulations, 2025

2025 Recovery of Penalty Regulations

- These Regulations replace the 2011 regulations.
- “person in default" has been included within the scope of the Regulations.
- The rate of interest on penalty has been reduced from 1.5% to 1%.
- Legal heirs of the person in default can be liable to pay penalty to the CCI.
- Regulation 10 now clarifies that if the person or enterprise in default fails to pay the penalty within the time stipulated in the recovery certificate, the recovery officer may simultaneously proceed to recover the penalty through attachment or sale of movable or immovable property.
- Regulation 11 now clarifies that when Income-tax authorities initiate proceedings (on reference by the CCI), the CCI’s recovery proceedings shall stand deferred indefinitely.

Competition Commission of India (Manner of Recovery of Monetary Penalty) Regulations, 2025

EUROPE

Regulatory

The European Data Protection Board (EDPB) publishes final guidelines on data transfer to third world-country authorities and introduces the Special Pool of Experts (SPE) training material on AI and data protection.

During its latest plenary, the European Data Protection Board (EDPB) adopted the final version of its guidelines on Article 48 of GDPR about data transfers to third country authorities, after public consultation. In addition, the Board presented two new Support Pool of Experts (SPE) projects, providing training material on artificial intelligence and data protection. Finally, the Board discussed the European Commission's request for a joint EDPB-EDPS opinion on the draft proposal on the simplification of record-keeping obligation under the GDPR.

Simplification of record-keeping obligation: EDPB and EDPS adopt letter to EU Commission

On 8 May, the EDPB and EDPS expressed preliminary support for the EU Commission's proposal to simplify record-keeping under Article 30(5) GDPR for smaller organizations. They emphasized that other GDPR duties remain and called for a careful impact assessment to ensure a balanced approach.

EDPB adopts guidelines on processing personal data through blockchains and is ready to cooperate with AI office on guidelines on AI act and EU data protection law.

On 14 April 2025, the EDPB adopted guidelines on personal data processing via blockchain, emphasizing GDPR compliance, early-stage data protection measures, clarity of actor roles, the need for DPIAs, and minimizing data storage on-chain. Public consultation runs until 9 June 2025.

EDPB adopts statement on age assurance, creates a task force on AI enforcement and gives recommendation to WADA

In February 2025, the EDPB adopted principles for age assurance to protect minors' data, expanded its ChatGPT taskforce to cover AI enforcement, and issued recommendations ensuring GDPR compliance in the 2027 WADA Anti-Doping Code.

Judgments

The French SA fines Caloga €80 000 - Judgment dated 15.05.2025

The CNIL (France's data protection authority) investigated Caloga, a data broker, as part of its 2022 focus on commercial prospecting practices. Caloga obtained personal data from other brokers and game/product websites (primary data collectors) to send marketing emails or share the data with third parties for the same purpose.

Key Violations Found	Decision
• **No valid consent** was obtained for email marketing (violating Article L.34-5 CPCE & GDPR), as consent forms were misleading. • **Difficult unsubscription** process, making withdrawal of consent harder than giving it. • **Lack of legal basis** for sharing data; Caloga wrongly relied on "legitimate interest" instead of consent. • **Excessive data retention**—data was stored indefinitely, extended every time an email was opened, even accidentally.	CNIL fined Caloga **€80,000**, citing the scale of data misuse, financial gain, and the company's market position. The fine was made public despite Caloga ceasing operations in 2024.

EUROPE

Judgments

The French SA fines Solocal €900 000- Judgement dated 15.05.2025
In 2022, the French Supervisory Authority (SA) investigated Solocal Marketing Services, a data broker involved in large-scale commercial prospecting via SMS and email. The Company sourced personal data from other brokers and contest/product sites (primary data collectors) and shared it with clients for marketing by phone or post.

Key Violations Found	Decision
• **Lack of valid consent** for electronic marketing due to misleading data collection forms (violating Article L.34-5 CPCE & GDPR). • **Inability to prove consent**—the company failed to show that individuals had agreed to data processing (violating Article 7 GDPR).	Solocal was fined **€900,000** and ordered to stop electronic marketing without valid consent. A **€10,000 daily penalty** was imposed for non-compliance after 9 months. The fine reflected the scale of violations, financial gain, and partial compliance after the investigation.

AI: the Italian Supervisory Authority fines company behind chatbot "Replika"- Judgement dated 10.04.2025
The Italian Supervisory Authority (SA) investigated Luka Inc. over its AI chatbot Replika, following media reports. The chatbot allowed users to create virtual companions with written and voice interactions.

Key Violations Found	Decision
No valid **legal basis** for data processing. **Inadequate privacy policy** and **no effective age verification**, despite excluding minors.	Luka Inc. was fined **€5 million** for multiple GDPR breaches and ordered to comply with data protection rules. Further investigations into its data processing practices may follow.

Slovenian SA: schools must adhere to principle of data protection and privacy by design. - Judgment dated 27.02.2025
The Slovenian Supervisory Authority investigated a school after a data breach involving its external meal service provider, which accessed the full student database, including sensitive data like subsidies despite only needing basic information.

Key Violations Found	Decision
• **Excessive data access** granted to the provider. • **Lack of data protection by design/default** (Article 25 GDPR). • **Inadequate risk assessment** and long-term corrective measures.	The school and its principal received a formal reprimand. The court upheld the decision, stressing that proper data protection practices could have prevented the breach and related risks.

EUROPE

Judgments

Polish SA: lack of procedures to protect personal data processed by the press- administrative fine of €13 500- Judgment dated 06.03.2025

In 2022, Polskie Radio Szczecin published an article revealing the identity of a minor victim of sexual harassment, who later died by suicide.

Key Violations Found	Decision
No **risk analysis** or **data security measures** and failure to follow internal **data protection procedures**.	A **€13,500 fine** was issued under GDPR Articles 24(1) and 32(1,2), with **60 days** to correct the shortcomings.

Polish SA: administrative fines for GDPR infringements where organising elections by postal vote between 2020- 23 for Minister of Digital Affairs to the extent of € 757 and for the Polish post to the extent of € 6 444 174 - Judgment dated 17.03.2025

In April 2020, during preparations for postal voting in Poland's presidential election, the Polish Post unlawfully processed data of 30 million citizens from the PESEL register, without a legal basis.

Key Violations Found	Decision
• Illegal Data Sharing • **Breach of GDPR** (Article 5 & 6) • **Mass data misuse** affecting nearly 30 Million citizens • **Delayed Data disposal**	Polish Post fined €6.44 million and the Minister of Digital Affairs fined €23,757. Violations: Articles 5(1)(a) & 6(3) GDPR.

USA

Regulatory

Trump orders full access to agency data for designated officials

President Donald Trump issued an executive order requiring all federal agencies to grant designated officials full access to unclassified records, data, software, and IT systems to identify and eliminate waste, fraud, and abuse. The order mandates the removal of internal barriers to data sharing and compels agencies to revise relevant regulations within 30 days. It also extends to state-run federally funded programs and third-party data holders. The directive follows Trump's earlier establishment of the Department of Government Efficiency Service (DOGE), which has already gained access to various sensitive federal systems. The order has raised concerns about privacy and the circumvention of existing data protection protocols, particularly after a DOGE official was implicated in improper data sharing.

AT&T data leak: 86 Million records exposed in latest alleged breach

In May 2025, about 86 million AT&T customer records, including 44 million Social Security Numbers in plain text, were leaked on a Russian cybercrime forum. The leak may be linked to a 2024 Snowflake breach but contains raw personal data without call metadata. This may be a new or combined leak from past breaches. AT&T had previous breaches in 2021 and 2024, but SSNs were encrypted until now. Experts warn this exposure greatly increases identity theft risks. AT&T is investigating the leak and noted cybercriminals often repackage old data for profit. The incident highlights ongoing cybersecurity challenges and the vulnerabilities of relying on SSNs for identity.

Apple's 95 million Siri settlement Apple will pay $95 million to settle claims that Siri recorded private conversations without consent. Though Apple denies wrongdoing, the case followed 2019 reports of accidental Siri activations.

Who's Eligible? U.S. users who owned Siri-enabled devices (iPhone, iPad, Mac, etc.) between September 17, 2014 – Dec 31, 2024.

Compensation: Up to $100, about $20 per device (maximum 5)

Claim deadline: July 2, 2025

Final hearing: August 1, 2025.

Claims can be filed via a notice email/postcard or through the official settlement website.

Judgments

Privacy and Hunger groups sue over USDA attempt to collect personal data of SNAP recipients.

Privacy and hunger relief organizations, along with several Supplemental Nutrition Assistance Program (SNAP) recipients, have filed a lawsuit against the U.S. Department of Agriculture in Washington, D.C. The suit alleges that the agency violated federal privacy laws by ordering states and vendors to hand over five years' worth of sensitive personal data including names, birth dates, addresses, and Social Security numbers of SNAP applicants and beneficiaries.

The plaintiffs, including the Electronic Privacy Information Centre and Mazon Inc., argue that this move disregards long-standing privacy protections and exploits vulnerable individuals relying on food assistance. SNAP, which supports over 42 million Americans, is federally funded but administered by states, which collect vast amounts of personal and financial data. The lawsuit seeks to prevent the federal government from misusing this sensitive information.

CANADA

Regulatory

The Privacy Commissioner of Canada, Philippe Dufresne, has launched an investigation into a privacy breach at Nova Scotia Power, a subsidiary of Emera Inc., under the Personal Information Protection and Electronic Documents Act (PIPEDA). Nova Scotia Power reported the breach and informed the Commissioner's office. Following complaints received, the Office is ensuring the company takes appropriate steps, including containment, customer notification, and risk mitigation. Affected individuals are being notified and offered two years of free credit monitoring. The Commissioner advises individuals to take protective actions such as changing passwords, monitoring accounts, and contacting financial institutions. He also stresses the importance of prioritizing cybersecurity in light of the increasing frequency and severity of cyberattacks.

OTHER COUNTRIES

Regulatory

DeepSeek shared user data with TikTok owner ByteDance (South Korea)

South Korea has accused Chinese AI startup DeepSeek of sharing user data with ByteDance, the parent company of TikTok. The Personal Information Protection Commission (PIPC) confirmed communication between the two entities, prompting the removal of DeepSeek from app stores in South Korea due to data protection concerns. While over a million downloads had occurred before the takedown, existing users can still access the app via browsers. Although a data link is confirmed, the extent and nature of the data shared remain unverified. This follows broader global concerns over Chinese data practices and surveillance laws, especially amid DeepSeek's rapid rise and parallels to previous TikTok-related privacy debates.

INDIA

Regulatory

The Ministry of Electronics and Information Technology (MeitY) released the draft Digital Personal Data Protection Bill, 2025 on 3rd January 2025.

MeitY has also invited comments from stakeholders which was closed in March.

It is expected that the final Rules will be placed before the Parliament during the monsoon session

BUSINESS REQUIREMENT DOCUMENT FOR CONSENT MANAGEMENT UNDER THE DPDP ACT, 2023

Launch of the Consent Management System (CMS) under the DPDP Act, 2023
The Business Requirement Document serves as a guideline for the development of a system that empowers Data Principals to exercise their rights over their personal data.

What is the Consent Management System?
The CMS is a secure, transparent, and user-friendly platform that manages the entire lifecycle of consent for personal data processing. It ensures that all data-related activities adhere to the principles of purpose limitation, data minimization, and user empowerment as mandated under the DPDP Act.

Key Features of CMS

Consent Collection
- Purpose-Specific and Granular Consent.
- User Interface and Accessibility.
- Explicit
- User Action: Consent must be given via affirmative action (e.g., "I Agree"), with no pre-checked boxes.
- Metadata Logging and Consent Artifact: CMS generates and stores consent artifacts (timestamp, user ID, purpose ID, consent status) in a secure, immutable format.
- Real-Time Sync & Acknowledgement.
- Audit Trail: All actions are logged for compliance audits.

Consent Validation to include:
- Pre-Processing Consent Check
- Scope Enforcement
- Real-Time API Validation
- Outcome Responses
- Audit Logging
- Error Notification

Consent Update
- Triggered by DF or User: Updates may be required due to added/changed data processing purposes, initiated by either Data Fiduciary or Data Principal.
- Notification & Transparency: Users are notified of changes in purpose/scope and prompted for updated consent with clear implications.
- Granular Updates: Users can update specific purposes while leaving others unchanged.
- Consent Artifact Modification: CMS updates the consent artifact, generates new timestamps, and logs the action.
- Sync & Notifications: Updated consents are synced across all relevant DF systems; users and stakeholders are notified immediately.
- Audit Logging: Every update is recorded with metadata for compliance tracking.

Consent Renewal
- Trigger Based on Expiry: Consent renewals are initiated when prior consents approach expiry. CMS must notify users 30 days before expiry.
- User Action Required: Renewals require affirmative user action (no auto-renewal).
- Display of Current Consents: CMS shows active consents, purposes, and expiration dates to assist decision-making.
- Consent Artifact Renewal: CMS updates the artifact with new status and logs changes.
- Real-Time Update to DFs: Renewed consents are synced immediately with all stakeholders.
- Audit Logging: Each renewal is recorded with user ID, purpose ID, timestamp, and new validity terms.

Consent Withdrawal
- Ease of Withdrawal: Must be as simple as the original consent process, accessible via dashboard or integrated platforms.
- Immediate Cessation: Data processing for the withdrawn purpose must stop immediately across all systems and third-party processors.
- Confirmation and Implications: Users must be informed of the withdrawal implications (e.g., loss of features) and receive confirmation.
- Legal Exceptions: Withdrawal does not apply if processing is mandated by law (e.g., regulatory compliance).
- Consent Artifact Update: Consent record is marked "Withdrawn" with timestamp; action logged immutably.
- Notification: DFs and Processors must be informed immediately of the withdrawal for operational enforcement

COOKIE CONSENT

Cookie consent lets the Data Principals informed of the tracking technologies and cookies used on the websites they visit and use. Shadowing the above principles, cookie consent can also be granted, modified or withdrawn.

Some of the main features of cookie consent are as follows:

- Granular consent options: Allows users to consent to specific categories of cookies tailored to the website and explicit consent to be obtained unless enabling of certain cookies are essential.
- Real-time updates: Allows users to modify or revoke cookie consent through a dedicated cookie preferences interface and updates users on change of cookie policies and request for renewed consent.
- Cookie policy display: Provides a clear and accessible cookie policy in the form of a banner, informing users of cookie usage on their first website visit.
- Multi-language support: Ensures cookie notices are available in languages.
- Auto-expiry: Sets expiration periods for user preferences and cookies.

USER DASHBOARD UPDATE

The dashboard will allow users to view the history of all consent-related actions such as the following:

- View all active, expired, and withdrawn consents
- Access detailed metadata (timestamp, purpose, status)
- Search & filter by date, purpose, or status
- Download consent logs securely in PDF/CSV formats

Modify or revoke consent	**Raise Grievances or Data Requests**
• Update or revoke consent for specific purposes • Changes take effect immediately • Receive instant confirmation of updates	• Submit grievances on consent violations or data misuse • Request access, correction, or erasure of your data • Track progress in real-time • Get notified via email/SMS • Automatic escalation to the DPO if unresolved

CONSENT NOTIFICATIONS

User notifications

User notifications ensures that all three parties, i.e., Data principals, Data Fiduciaries and Data Processors are promptly aware of any sort of consent-related activity. User notifications notify the users on:

- Consent approvals or rejections
- Withdrawal confirmations
- Renewal reminders for expiring consents
- Status of data access, correction, or erasure requests

Data Fiduciary & Processor Alerts

The aim of this feature is to alert Data Fiduciary and Data Processor about consent updates, withdrawals or validation requests to ensure compliance.

Key Alerts:

- Consent withdrawals or expirations
- New or updated consents
- Compliance alerts triggered by the system

COOKIE CONSENT

Grievance Redressal Mechanism

This mechanism ensures that Data principals are able to report and file complaints regarding data processing, privacy violation or consent management issues.

Complaint lodging (Key features)

- Registers complaints against data misuse, consent violation and/or data handling.
- User-friendly and multilingual interface.
- Generates a unique reference ID for tracking.
- Complaints are encrypted and secure.

Resolution tracking

It provides updates on the status of the complaint. It displays real time status to the complainant and automatically escalates unresolved complaints. It maintains a detailed logs of actions taken and allow users to provide feedback on the resolution process. Once the complaint is resolved the system updates the status to “closed” and sends a summary to the complainant.

SYSTEM ADMINISTRATION

This provides administrative capabilities to ensure secure and efficient operations of CMS. It includes managing user roles, configuring policies and maintaining compliance standards.

User role management

- Defines and manages access controls within the CMS
- Assigns permissions based on predefined roles
- Enables multi-level access and maintains logs of role assignments and customizations
- All time monitoring of activities

Data retention policy configuration

This policy ensures that personal data and consent records are retained or deleted based on predefined schedules. After configuring data as per the regulatory framework it notifies the user and maintains a record for all data retention. The admin defines data retention policies, specifying retention policies for different categories then the CMS enforces policies triggering deletion workflows for expired records. Then the system identifies records exempted from deletion due to legal requirements.

LOGGING

Logging ensures all consent-related activities within CMS are documented in transparent, secure and tamper-proof manner and provides an immutable trail for compliance verification and audits as mandated by the DPDP Act.

- Comprehensive Loggin which records every consent action including consent grant, update and withdrawal followed by User ID, Purpose ID and consent status. Notifications are sent to Data fiduciaries and acknowledgement receipts are produced.
- Audit Readiness maintains audit logs in a structured format, easy retrieval and reporting. Ensures logs are maintained as per the regulatory requirements.
- Access Control by restricting access with the use of Role-based Access Control and Multi-Factor Authentication.

THANK YOU

For further queries/information please get in touch with us

SHIVADASS & SHIVADASS®
LAW CHAMBERS

Level 3,
No. 4/2, Millers Road,
Bangalore – 560052
admin@sdlaw.co.in | +91 8043779955