SILICON COMNET PRIVATE LIMITED · Volume 1, Issue 1 · May 2026

The SCPL Privacy Review

Enforcement & Compliance Intelligence — Monthly Review

Covering 1 May – 31 May 2026 · Cross-border transfers · Consumer privacy · Financial services · Children's data · DPDP Act 2023

About Silicon Comnet Private Limited

Silicon Comnet Private Limited (SCPL) is a cybersecurity and data protection advisory firm serving enterprises, financial institutions, and digital platforms across India and globally. SCPL is part of the OACPL Group, which brings over 30 years of combined experience in networks, telecommunications, systems, and applications; SCPL itself is built around a dedicated team of practitioners, researchers, and analysts specialising in cyber risk, data governance, privacy, and regulatory compliance.

SCPL delivers a comprehensive portfolio of cybersecurity services, including cyber exposure management, adversarial security testing, data-centric security solutions, managed security services, incident response, cyber forensics, and offensive security. The firm also offers globally recognised EC-Council-certified training programs, including CEH, CSA, and ECIH, helping organisations strengthen their security capabilities and workforce readiness.

In the area of data protection and privacy, SCPL provides end-to-end advisory, assessment, remediation, and implementation services aligned with India's Digital Personal Data Protection Act, 2023, the DPDP Rules, 2025, and global frameworks such as GDPR, ISO 27001, and SOC 2. Its services include privacy gap assessments, implementation, privacy control frameworks, Records of Processing Activities (RoPA), Data Processing Agreements (DPAs), DPIAs/PIAs, consent management frameworks, data breach response programs, and DPO-as-a-Service offerings.

SCPL has successfully delivered cybersecurity and privacy engagements across diverse sectors, including BFSI, IT/ITES, manufacturing, cloud-native businesses, and aviation, helping organisations strengthen resilience, manage regulatory obligations, and build trust in an increasingly digital environment.

Led by professionals from IIT Delhi and IIM Ahmedabad, alongside former leaders from Cisco, BT, Verizon, and Check Point, SCPL combines deep technical expertise with strong legal and regulatory insight, enabling organisations to

CYBERSECURITY

— Cyber Exposure Management

— Adversarial Security Testing

— Data Centric Security Solutions

— Managed Security Services

— EC-Council Training (CEH, CSA, ECIH)

DATA PROTECTION & COMPLIANCE

— DPDP Act 2023 / DPDP Rules 2025

— GDPR, ISO 27001 & SOC 2

— Gap Assessments & Privacy Frameworks

— RoPA, DPA, DPIA / PIA

— Consent Management

— DPO-as-a-Service & Breach Response

CONTACT

www.siliconcomnet.com
reach@siliconcomnet.com
+91 9311 425007
16/8, 3rd Floor, Arya Samaj Road,
Karol Bagh, New Delhi — 110005
C-43, 2nd Floor, Sector 8, Noida

secure critical digital assets while meeting evolving compliance and privacy requirements.

The SCPL Privacy Review is Silicon Comnet's monthly enforcement digest, tracking major enforcement actions, regulatory investigations, significant data breaches and emerging privacy trends so that Indian and global organisations can act before enforcement reaches them.

SECTION I — FINES, ORDERS & INVESTIGATIONS: MAY 2026

This section covers ten enforcement actions issued or announced during May 2026.

01. MLU B.V. (Yango/Yandex Group)

€100,000,000

Netherlands · Finland · Norway · Autoriteit Persoonsgegevens (Dutch AP) + Finnish Data Protection Ombudsman + Norwegian Datatilsynet · *8 May 2026*

The Autoriteit Persoonsgegevens of the Netherlands, jointly with data protection regulators in Finland and Norway, imposed a €100 million fine on MLU B.V., the Netherlands-registered European operator of the Yango ride-hailing app, part of the Yandex Group, for unlawfully transferring personal data of Finnish and Norwegian passengers and drivers to servers in Russia.

The investigation, initiated in late 2023 following alerts from Finnish and Norwegian regulators, found that Yango had been continuously transferring sensitive personal data to Russia since at least 23 May 2022. The data included driving licence scans, home addresses, bank account numbers, social security numbers, precise trip location histories, chat messages, and photographs. Notably, MLU had put EU Standard Contractual Clauses (SCCs) in place for the transfers; the AP found these insufficient in practice, given Russia's surveillance and government-access regime and the absence of an independent data protection authority, meaning the transfers could not be treated as compliant with Articles 44–46 of the GDPR. The decision is dated 1 April 2026 and was publicly announced on 8 May 2026. The fine of €100 million was calculated on Yandex Group's global turnover of approximately €12 billion. An immediate cessation order was also issued. MLU has stated it will challenge the decision.

> **India / DPDP Act 2023 - Compliance Angle:** Section 16 of the DPDP Act 2023 empowers the Central Government to restrict the transfer of personal data to specified countries or territories notified by the government, a blacklist-style mechanism that differs from the GDPR's adequacy and SCC-based regime. The Yango case is nonetheless instructive: MLU had executed SCCs, and the AP still found the transfer unlawful because the destination country's surveillance regime made the contractual safeguard ineffective in practice. Indian data fiduciaries should treat contractual paperwork as necessary but not sufficient, and should map all offshore transfer destinations and assess the real-

world risk of government access before the DPDP Act's penalty provisions become enforceable in May 2027.

Primary Source: Dutch AP, Official Decision & Press Release, 8 May 2026 · **News Coverage:** ICLG: Taxi App Fined €100M over Russian Data Transfers

02. Permanent TSB (PTSB)

€277,500

Ireland · Data Protection Commission (DPC) · *8 May 2026*

On 8 May 2026, Ireland's Data Protection Commission announced its final decision following a GDPR inquiry into a series of personal data breaches at Permanent TSB (PTSB), one of Ireland's principal retail banks. The DPC imposed a total fine of €277,500 and issued a formal reprimand.

The breaches, first reported to the DPC in May 2022, occurred when malicious actors who held certain customer information called PTSB's Open24 Contact Centre, impersonated account holders, bypassed identity verification, changed account details, and obtained additional account information. In all three incidents, appropriate security protocols were not followed. Affected customers were exposed to increased fraud risk, some were forced to close their accounts, and some suffered direct financial loss.

The DPC found three GDPR violations: (i) infringement of Article 5(1)(f), failure to ensure appropriate security of customer personal data using adequate technical and organisational measures (TOMs); (ii) infringement of Article 32(1), failure to implement TOMs appropriate to the level of risk within the Open24 Contact Centre; and (iii) infringement of Article 33(1), failure to notify the DPC within 72 hours of becoming aware of the breaches. The DPC fined PTSB €250,000 for the Article 5 and 32 violations and €27,500 for the Article 33 breach notification failure.

India / DPDP Act 2023 - Compliance Angle: Under DPDP Act 2023 Section 8(6), data fiduciaries must notify the Data Protection Board of India of any personal data breach 'in such form and manner as may be prescribed'. The PTSB case shows how a contact-centre identity verification failure, not a technical cyberattack, became a GDPR breach notification violation. Indian banks, NBFCs, and customer-service operations must review both their authentication controls and their internal breach escalation timelines to ensure 72-hour-equivalent notification is operationally achievable.

Primary Source: Irish DPC, Official Decision Announcement, 8 May 2026 · **News Coverage:** RTÉ News: PTSB fined €277,500 by Data Protection Commission

03. General Motors LLC & OnStar

USD $12,750,000

California, United States · California AG (Rob Bonta) + California Privacy Protection Agency (CPPA) · *8 May 2026*

On 8 May 2026, California Attorney General Rob Bonta, together with the California Privacy Protection Agency and the District Attorneys of Los Angeles, San Francisco, Napa, and Sonoma counties, announced a $12.75 million settlement with General Motors and its subsidiary OnStar. The settlement resolves a civil lawsuit alleging violations of the California Consumer Privacy Act (CCPA), the California Unfair Competition Law, and the California False Advertising Law, and is described by the parties as the largest CCPA-related enforcement penalty to date.

Between 2020 and 2024, GM collected geolocation data, driving behaviour metrics (hard braking, rapid acceleration, seatbelt usage, speed thresholds, late-night driving frequency), and personal details of hundreds of thousands of California consumers through OnStar's connected-vehicle platform. GM then sold this data to two data brokers, Verisk Analytics and LexisNexis Risk Solutions, for insurance-underwriting purposes, without adequate consumer notice or consent. The data had originally been collected for safety and navigation purposes only. Some consumers saw their insurance premiums rise directly as a result.

Under the settlement, GM must: pay $12.75 million in civil penalties; cease selling driving behaviour data to consumer reporting agencies for five years; delete all retained driving data within 180 days, absent fresh affirmative consent; request LexisNexis and Verisk to delete GM-sourced data; and implement an auditable privacy programme with mandatory risk assessments. GM resolved the matter without admitting liability.

> **India / DPDP Act 2023 - Compliance Angle:** DPDP Act 2023 mandates purpose limitation: data collected for one purpose cannot be used for any other purpose without fresh, specific consent. The GM settlement is the most consequential global demonstration to date of what happens when companies quietly repurpose personal data, particularly behavioural and location data, for commercial ends undisclosed at collection. Indian data fiduciaries in automotive, IoT, healthcare, and fintech must audit whether any data collected for product or service delivery is being used for analytics, profiling, or third-party sale without valid consent.

Primary Source: California DOJ, Official Press Release, 8 May 2026 · **News Coverage:** IAPP: California authorities announce largest CCPA fine to date

04. South Staffordshire Plc & South Staffordshire Water Plc

£963,900

United Kingdom · Information Commissioner's Office (ICO) · *7 May 2026*

On 7 May 2026, the UK ICO imposed a fine of £963,900 on South Staffordshire Plc and its regulated water subsidiary, South Staffordshire Water Plc, for infringements of Articles 5(1)(f) and 32(1) of the UK GDPR arising from a major ransomware attack.

The attack began in September 2020 when an employee opened a malicious email attachment, installing software that gave the Cl0p ransomware group a persistent foothold on the corporate

network. The threat actor remained undetected for nearly two years, moving laterally using domain administrator credentials from May 2022. The intrusion was only discovered in July 2022 when IT performance issues prompted an internal investigation, and staff found a ransom note. Between August and November 2022, over 4.1 terabytes of stolen data were published on the dark web, including the personal information of 633,887 customers and employees: names, addresses, dates of birth, email addresses, National Insurance numbers, usernames, passwords, and account information.

The ICO found that South Staffordshire failed to implement adequate technical and organisational security measures, had no monitoring capable of detecting the intrusion for almost two years, and left domain administrator credentials inadequately protected. The fine reflects a voluntary settlement discount. Leigh Day law firm is currently acting for over 6,500 affected individuals in compensation claims.

> **India / DPDP Act 2023 - Compliance Angle:** This case is a direct illustration of DPDP Act 2023 Section 8(5), which requires data fiduciaries to implement 'reasonable security safeguards to prevent personal data breach'. The ICO's finding, that a two-year undetected intrusion represented a failure of security obligation, establishes that passive security (firewalls, perimeter controls) is insufficient. Active monitoring, anomaly detection, and tested incident response plans are now standard regulatory expectations under UK GDPR and should be treated as such under India's DPDP framework.

Primary Source: ICO Official Enforcement Notice, 7 May 2026 · **News Coverage:** Burges Salmon: Key takeaways from the South Staffordshire fine

05. Infinite Styles Services Co. Ltd. (SHEIN Ireland)

Formal Inquiry Opened

Ireland (Lead EU Supervisory Authority) · Data Protection Commission (DPC) · *5 May 2026*

Ireland's Data Protection Commission opened a formal statutory inquiry into Infinite Styles Services Co. Ltd., the Dublin-based EMEA entity of fast-fashion retailer SHEIN, under Section 110 of the Data Protection Act 2018, and announced the inquiry publicly on 5 May 2026.

The inquiry will examine whether SHEIN's transfers of EU and EEA user personal data to China comply with GDPR's international transfer framework (Articles 44–46) and whether SHEIN's transparency disclosures under Articles 5 and 13 are adequate. DPC Deputy Commissioner Graham Doyle stated: 'Recent regulatory action by the DPC, together with complaints to other European supervisory authorities, has brought data transfers to China, in particular, into focus. The inquiry is an important strategic priority for the DPC.'

The inquiry follows directly from the DPC's €530 million fine against TikTok in May 2025 for identical conduct, unlawful EEA-to-China data transfers. The DPC has made explicit its intention to extend China-transfer scrutiny from social media to e-commerce. No fine has yet been issued; enforcement measures will follow if breaches are found. SHEIN stated it takes its obligations 'extremely seriously' and is engaging with the DPC.

> **India / DPDP Act 2023 - Compliance Angle:** While the SHEIN inquiry concerns the EU's adequacy-based transfer regime, India's approach under Section 16 of the DPDP Act 2023 is a notified-country (negative-list) model rather than an adequacy assessment. The transparency question at the centre of the DPC inquiry, whether disclosures under Articles 5 and 13 GDPR accurately describe cross-border data flows, mirrors the notice obligations under Section 5 of the DPDP Act 2023. Indian e-commerce and retail platforms that route order, payment, or identity-verification data to fulfilment or customer-service operations outside India should ensure their consent notices accurately describe these transfers and confirm that no DPDP-notified country restrictions apply.

Primary Source: Irish DPC — Official Announcement, 5 May 2026 · **News Coverage:** RTÉ News: Irish data watchdog opens investigation into Shein

06. Isabel SA (TruliUs Platform)

€120,000

Belgium · Autorité de Protection des Données (APD), Decision No. 103/2026 · *12 May 2026*

On 12 May 2026, Belgium's APD issued Decision No. 103/2026 fining Isabel SA, a B2B platform provider operating the TruliUs corporate identity verification service, €120,000 for multiple GDPR violations arising from a fundamental data-controller misclassification.

The APD found that Isabel SA had classified itself as a data processor in its terms and conditions, when in fact, because the company independently designed the system's architecture and defined all data processing parameters, it was the data controller. This misclassification produced cascading violations: (i) excessive collection of identity attributes beyond what necessity required; (ii) an inaccurate privacy policy that did not reflect real processing practices; and (iii) failure to respond to data subject access requests within the GDPR-mandated timeframe, due to an internal technical failure. The €120,000 penalty reflects the severity of the controller-versus-processor misclassification as a structural compliance failure.

> **India / DPDP Act 2023 - Compliance Angle:** Under DPDP Act 2023, distinguishing between a Data Fiduciary (controller equivalent) and a Data Processor is foundational: only Data Fiduciaries bear direct statutory obligations, including under Sections 8 and 9. The Isabel SA case shows how misclassifying yourself as a processor, when you are actually determining the purposes and means of processing, creates a compounding compliance gap that exposes the organisation to transparency, necessity, and data-subject rights simultaneously.

Primary Source: Belgian APD, Decision No. 103/2026, 12 May 2026 · **News Coverage:** DataGuidance: Belgium, Belgian DPA fines Isabel SA €120,000

07. Société Wallonne des Eaux (SWDE)

€86,000

Belgium · Autorité de Protection des Données (APD), Decision No. 102/2026 · *12 May 2026*

Belgium's APD published Decision No. 102/2026 on 12 May 2026, fining SWDE, the Walloon public water utility serving approximately 2.4 million people, €86,000 for multiple GDPR and Belgian Electronic Communications Act violations arising from its customer service call-recording practices. The case was initiated by an employee complaint filed in April 2020.

The APD found four violations: (i) call recordings made without a valid legal basis under GDPR Article 6; (ii) failure to proactively inform callers of recording under Articles 13 and 14, since the company made this information available only to callers with internet access; (iii) retention of test audio files indefinitely, without documented retention limits; and (iv) failure to put a formal data processing agreement in place with the third-party subcontractor that evaluated recordings over a five-year period, in breach of Article 28. The APD also ordered SWDE to bring its disclosures, opt-out mechanisms, retention configurations, and processor contracts into full compliance.

The case is notable because SWDE is a public-sector entity, confirming that state-owned utilities and public bodies are subject to the same GDPR enforcement intensity as private companies.

> **India / DPDP Act 2023 - Compliance Angle:** DPDP Act 2023 Section 5 requires a data fiduciary to give a notice to the data principal before or at the time of collecting personal data. Indian organisations recording calls for quality assurance or HR purposes must ensure: (a) callers are notified proactively and clearly before recording begins; (b) a legal basis (consent or legitimate use) is documented; and (c) any third-party processor analysing those recordings has a formal Data Processing Agreement in place.

Primary Source: Belgian APD, Decision No. 102/2026, 12 May 2026 · **News Coverage:** Data Guidance: Belgium - Belgian DPA fines SWDE €86,000

08. Unnamed Technology Corporation (Belgium)

€177,000

Belgium · Autorité de Protection des Données (APD), Decision No. 101/2026 · *12 May 2026*

Also on 12 May 2026, the Belgian APD published Decision No. 101/2026, fining an unnamed large technology corporation €177,000 for unlawfully retaining and processing the email account of a former freelance consultant after her contract ended.

Rather than deleting the departed consultant's corporate email account after a brief transition window, the company maintained the inbox in 'backup status' and continued to process incoming third-party communications for more than a year, without legal basis. An automatic out-of-office reply also erroneously indicated to external contacts that the consultant's absence was temporary. When the former consultant filed a formal subject access request to review her personal data retained in the account, the company refused access, citing protection of

commercial trade secrets. The APD rejected this rationale and found it an unlawful obstruction of data subject rights under Articles 15 and 17 GDPR.

> **India / DPDP Act 2023 - Compliance Angle:** Under DPDP Act 2023 Section 8(7), a data fiduciary must erase personal data of a data principal as soon as it is reasonable to assume that the purpose for which the data was collected is no longer being served, and the data principal has not approached the fiduciary for the performance of any obligation. This Belgian case is a direct illustration: employment and contractor data must be deleted when the professional relationship ends, absent a specific documented retention justification.

Primary Source: Belgian APD, Decision No. 101/2026, 12 May 2026 · **News Coverage:** Osano Enforcement Tracker: Belgium, unnamed technology corporation

09. Media Operators - Garlasco Case Coverage (Italy)

Formal Warning

Italy · Garante per la Protezione dei Dati Personali · *15 May 2026*

On 15 May 2026, Italy's Garante issued a formal warning and strict reminder to media operators that had broadcast audio and transcripts of private conversations between a criminal defendant and his defence counsel in connection with coverage of the Garlasco murder case.

The Garante found that broadcasting recordings of privileged attorney-client communications, strictly prohibited under Italian criminal procedure law, also breached the principle of 'essentiality of information' under Italian data protection law and the journalists' code of conduct, which implements the journalistic derogation in Article 85 of the GDPR and requires that media publish only personal data that is genuinely necessary for informing the public interest. The authority characterised the conduct as 'continuous and morbid sensationalism of criminal news', finding that the broadcasts exceeded legitimate journalistic purposes and compromised individual dignity. The Garante emphasised that media freedom does not licence publishing personal data, particularly sensitive communications, beyond the threshold of genuine public interest.

> **India / DPDP Act 2023 - Compliance Angle:** Unlike the GDPR, which carves out journalistic processing under Article 85, the DPDP Act 2023 contains no dedicated journalistic exemption. Section 17 permits the Central Government to exempt specified classes of data fiduciaries by notification, and industry bodies such as the Editors Guild of India have sought such a notification for journalistic activity, but none has been issued to date, and the scope of journalistic processing under the Act remains contested and is the subject of pending litigation. The Garante's 'essentiality of information' principle, that only data genuinely necessary for public interest journalism may be processed, is a useful proportionality benchmark for Indian media organisations and digital publishers to apply voluntarily while this gap in the Indian framework remains

> unresolved, particularly when handling personal data of individuals involved in legal proceedings.

Primary Source: Garante - Official Decision, 15 May 2026 · **News Coverage:** Osano Enforcement Tracker: Italy - Media / Garlasco Case

10. Roblox Corporation

Investigation Opened

Connecticut, United States · Connecticut Attorney General (William Tong) · *26 May 2026*

On 26 May 2026, Connecticut Attorney General William Tong announced a formal investigation into Roblox Corporation following reports alleging that the platform has been used to facilitate harm to children, including child exploitation. The investigation will examine what Roblox knew about alleged child exploitation on its platform; whether and how it may have benefited financially from such activity; and what protective measures Roblox has taken or failed to take to safeguard child users. No findings have yet been made.

The investigation is part of a coordinated multi-state regulatory push targeting digital platforms serving minors, and follows directly from the UK ICO's £14.47 million fine against Reddit in February 2026 for age-assurance failures affecting children under 13. Children's data safety has emerged as the fastest-growing enforcement category globally in 2026, with regulators in the US, EU, and UK all explicitly prioritising it. No fine has been issued yet; the investigation may result in civil enforcement under Connecticut's CTDPA and other applicable laws.

> **India / DPDP Act 2023 - Compliance Angle:** Section 9 of the DPDP Act 2023 requires verifiable parental consent before processing personal data of any child (under 18) and prohibits processing that is likely to cause detrimental effects on the well-being of the child. Indian EdTech, gaming, social, and consumer platforms must treat children's data compliance as a pre-enforcement imperative, not a deferred obligation. Under the Schedule to the DPDP Act 2023, non-compliance with Section 9 can attract a penalty of up to ₹200 crore.

Primary Source: Connecticut AG - Official Announcement, 26 May 2026 · **News Coverage:** DataGuidance: Connecticut AG announces investigation into Roblox

SECTION II — Q1 2026 ENFORCEMENT: ESSENTIAL CONTEXT FOR MAY

Three major enforcement decisions finalised in Q1 2026 shaped the regulatory environment in which May's actions were issued. Each is included with its primary DPA source.

Intesa Sanpaolo - Italy | Garante

€49.4M (Two Fines)

12 March 2026 (€17.6M) and 30 March 2026 (€31.8M) · Italy's largest bank

The Garante issued two fines in under three weeks. The first (€17.6M, 12 March) penalised the bank for unlawfully profiling 2.4 million customers, using undisclosed algorithmic criteria, to select them for migration to its digital-only subsidiary Isybank, without valid legal basis or transparency. The second (€31.8M, 30 March) arose from an insider breach: one employee accessed the private banking records of 3,573 customers, including senior politicians and public officials, 6,600 times between 2022 and 2024, entirely undetected by the bank's access control and monitoring systems.

> **India / DPDP Act 2023 - Compliance Angle:** DPDP Act 2023 Section 8(5) requires data fiduciaries to implement reasonable security safeguards to prevent personal data breaches — including insider access. Role-based access controls, access logging, and anomaly detection must be treated as statutory compliance measures, not optional security enhancements.

Primary Source: Garante - Decision No. 163 (12 March 2026) · **Analysis:** Captain Compliance: Italian DPA Slaps Intesa Sanpaolo

Reddit, Inc. | UK ICO

£14,470,000

24 February 2026 · United Kingdom · Information Commissioner's Office

The ICO fined Reddit £14.47 million, its third-largest penalty to date, for unlawfully processing personal data of children under 13 for nearly seven years. Reddit's Terms of Service prohibited under-13 users but relied solely on unverified self-declaration of age, with no technical age-assurance mechanism, until July 2025. The ICO found no valid lawful basis for processing children's data, no DPIA, and no meaningful application of the UK's Children's Code. The fine was reduced from £24 million in recognition of Reddit's cooperation and remediation steps. Reddit has indicated it will appeal.

> **India / DPDP Act 2023 - Compliance Angle:** DPDP Act 2023 Section 9 requires verifiable parental consent before processing data of a child under 18 and prohibits processing likely to cause detrimental effects on the child's wellbeing. 'Verifiable' is the operative word — self-declaration will not be sufficient under a DPDP enforcement regime. Indian digital platforms must implement age-assurance mechanisms now.

Primary Source: ICO - Official Press Release, 24 February 2026 · **Analysis:** Hunton: UK ICO Fines Reddit £14.47 Million

Free Mobile & Free SAS (Iliad Group) | CNIL France

€42,000,000

13 January 2026 · Free Mobile (€27M) + Free SAS (€15M)

The CNIL fined both Iliad Group subsidiaries following an October 2024 data breach that exposed the personal data, including bank IBANs, of 24 million subscribers. Three violations were found: (i) inadequate VPN authentication, making the breach possible; (ii) failure to adequately notify

affected individuals of the breach risks; and (iii) excessive retention of former subscribers' data. Iliad Group has said it will appeal to the Conseil d'État.

> **India / DPDP Act 2023 - Compliance Angle:** DPDP Act 2023 Section 8(5) and (6): telecom and ISP companies in India must implement security measures commensurate with risk, including remote-access authentication, and must notify the DPBI and affected data principals of breaches in the prescribed form and timeline. The CNIL's finding that IBAN data was exposed through a remote-access weakness is directly applicable to Indian telecom companies managing subscriber databases.

Primary Source: CNIL — Official Decision, 13 January 2026 · **Analysis:** The Record: France fines telcos €42M after 2024 breach

SECTION III — INDIA: DPDP ACT 2023 ENFORCEMENT COUNTDOWN

India's Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025. The Data Protection Board of India (DPBI) is now constituted. Full substantive enforcement, including penalty provisions, is scheduled to commence on 13 May 2027. The window for structured compliance action is therefore approximately twelve months.

Date	Milestone	Status
13 Nov 2025	DPDP Rules, 2025 notified; foundational provisions relating to the Data Protection Board of India (DPBI) came into force	✓ Done
Jun–Aug 2026	Expected operationalisation of the Consent Manager ecosystem (industry expectation, not a statutory deadline)	In Progress
13 Nov 2026	Rule 4 becomes effective – registration and obligations of Consent Managers become mandatory	Upcoming
13 May 2027	Remaining substantive provisions of the DPDP Rules become effective; full compliance expected and penalties become enforceable	Upcoming

Maximum Penalties Under DPDP Act 2023

Violation	Maximum Fine
Failure to implement security safeguards (Section 8(5))	Up to ₹250 Crore
Processing without valid consent / non-compliance with obligations relating to processing personal data (including Section 4 obligations)	Up to ₹200 Crore
Breach of children's data obligations (Section 9)	Up to ₹200 Crore

Failure to notify DPBI / data principal of a breach (Section 8(6))	**Up to ₹200 Crore**
Non-fulfilment of Significant Data Fiduciary (SDF) obligations (Section 10)	**Up to ₹150 Crore**
Failure to comply with obligations not specifically covered elsewhere in the Schedule (residuary category)	**Up to ₹50 Crore**

SECTION IV — SIX COMPLIANCE PRIORITIES FROM MAY 2026 ENFORCEMENT

1. Map and validate every cross-border data transfer

The Yango €100M fine and the DPC's SHEIN inquiry are both cross-border transfer violations. Every organisation must maintain a living map of all data flows, identify every transfer destination, and ensure that Standard Contractual Clauses or other lawful transfer mechanisms are in place and auditable before data leaves the jurisdiction.

2. Treat data minimisation and purpose limitation as active enforcement targets

The GM $12.75M settlement established data minimisation as a live enforcement priority under CCPA for the first time. Data collected for one stated purpose cannot be silently repurposed for analytics, profiling, or third-party sale. Organisations must audit every data category against its declared collection purpose and delete or anonymise anything that exceeds it.

3. Harden authentication and account-security controls at every customer channel

The PTSB €277,500 fine arose not from a technical hack but from social-engineering calls to a contact centre. Any customer-facing channel through which personal data can be accessed or modified, phone, chat, email, or portal, must have authentication controls and account-change protocols calibrated to the sensitivity of data at risk.

4. Implement active security monitoring and test incident response

South Staffordshire Water had hackers undetected for nearly two years. The ICO found this was a failure of organisational security measures, not simply bad luck. Active monitoring, anomaly detection, and tested incident response plans are now standard regulatory expectations. Passive perimeter security is insufficient.

5. Know whether you are a controller or a processor and document it correctly

The Isabel SA €120,000 fine arose from a misclassification of the company as a processor when it was in fact a controller. This single error produced cascading violations across necessity, transparency, and data subject rights. Every organisation handling personal data, including B2B technology platforms, must formally assess and document its controller or processor status for each processing activity.

6. Delete personal data of former employees and contractors promptly

The unnamed Belgian tech company's €177,000 fine arose from retaining and processing a departed freelancer's email for over a year with no legal basis. Organisations must have documented offboarding procedures that include email-account deletion timelines and

confirmation that access rights are revoked. Retention of former staff data 'just in case' is not a lawful basis under GDPR or DPDP.

About This Publication

The SCPL Privacy Review is published monthly by Silicon Comnet Private Limited. This publication is provided for informational purposes only and does not constitute legal, regulatory, cybersecurity, or professional advice. Readers should obtain specific advice before acting on any information contained herein.

Silicon Comnet Private Limited

16/8, 3rd Floor, Arya Samaj Road, Karol Bagh, New Delhi — 110005 · C-43, 2nd Floor, Sector 8, Noida

reach@siliconcomnet.com · +91 9311 425007

www.siliconcomnet.com