SILICON COMNET PRIVATE LIMITED · *Volume 1, Issue 2* · *June 2026*

The SCPL Privacy Review

Enforcement & Compliance Intelligence — Monthly Review

Covering 1 June – 30 June 2026 · Cross-border transfers · Children's data · Health & special-category data · Public-sector accountability · DPDP Act 2023

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, alongside globally recognised EC-Council-certified training programs (CEH, CSA, ECIH).

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. 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.

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.

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

SECTION I — FINES, ORDERS & INVESTIGATIONS: JUNE 2026

This section covers sixteen enforcement actions, rulings, complaints, and major incidents issued or announced during June 2026, sourced from DataGuidance and the underlying regulators.

01. TikTok Technology Limited - Irish High Court

€530,000,000 (Upheld)

Ireland · High Court of Ireland, on appeal from the Data Protection Commission (DPC)

The Irish High Court largely upheld the Data Protection Commission's May 2025 finding that TikTok infringed the GDPR through its transfers of EEA user data to China, confirming the €530 million fine (€485 million for the Article 46(1) transfer infringement and €45 million for the Article 13(1)(f) transparency infringement) and rejecting most of TikTok's grounds of appeal.

The Court did, however, send one element of the DPC's order back for reconsideration: the corrective order suspending future EEA-to-China transfers. According to DPC chair Des Hogan, the Court found that the DPC had not adequately set out in its decision how it had considered certain submissions made by TikTok, a procedural-fairness point rather than a finding that the underlying facts had changed. The DPC must now reassess that specific order; TikTok's separate appeal against the size of the fine has not yet been heard.

India / DPDP Act 2023 - Compliance Angle: The case is a reminder that a regulator's procedural obligation to engage with a respondent's submissions visibly is as consequential as the substantive finding itself. As the Data Protection Board of India develops its own adjudication practice ahead of 2027 enforcement, Indian data fiduciaries should expect that DPBI orders, and any future appeals of them, will turn partly on whether the Board's own reasoning record demonstrates genuine engagement with a fiduciary's defence, not merely a recitation of the alleged violation.

Primary Source: Irish Data Protection Commission — Decision, Inquiry into TikTok Technology Limited, 30 April 2025 (fine); High Court judgment 3 June 2026 · **News Coverage:** The Irish Times: Data Protection Commission reconsidering TikTok data-transfer ban after court ruling; https://www.arthurcox.com/knowledge/the-tiktok-decision-what-it-means-for-international-data-transfers/

02. X Corp. & X.AI LLC (Grok)

PIPEDA Breach Finding (No Monetary Penalty Available)

Canada · Office of the Privacy Commissioner of Canada (OPC)

Canada's Privacy Commissioner, Philippe Dufresne, released findings that X Corp. and xAI violated the Personal Information Protection and Electronic Documents Act (PIPEDA) by launching the Grok Imagine AI image-generation tool without adequate privacy safeguards or a timely privacy impact assessment. At its peak, the tool was used to generate more than 6,000 non-consensual sexualized deepfake images per hour, with the OPC recording 1.8 million sexualized images shared since 29 December 2025, including an estimated 23,000 images depicting children in an 11-day window.

The OPC found Grok Imagine's privacy impact assessment was not completed until March 2026, months after its July 2025 launch, and that the assessment did not accurately reflect the security, safety, and privacy risks involved. The Commissioner recommended xAI suspend the image generator entirely until adequate safeguards could be demonstrated; the companies refused, though they agreed to quarterly compliance reports and independent third-party audits. Dufresne publicly stated that Canada's privacy law does not currently give the OPC the power to fine companies or order a product suspended, and renewed his call for stronger enforcement powers comparable to other jurisdictions.

India / DPDP Act 2023 - Compliance Angle: This finding is one of the starkest illustrations globally of why DPDP Act 2023 Section 9's child-safety provisions and Section 8(5) security-safeguard obligations must be treated as pre-launch, not post-incident, requirements: a privacy assessment completed months after a generative AI feature already caused mass harm provides no protection at all. Indian

entities building or deploying generative image or video tools, especially those accessible to or usable by minors, must complete a documented risk assessment addressing foreseeable misuse (including non-consensual and child sexual abuse imagery) before public launch, not as a remedial step after harm is reported.

Primary Source: Office of the Privacy Commissioner of Canada — PIPEDA Findings #2026-004, 11 June 2026 · **News Coverage:** IAPP: OPC finds Grok chatbot and deepfakes violated Canada's privacy law

03. Coupang Corp. & Coupang Fulfilment Services

₩624.68 Billion (approx. US$409,000,000)

South Korea · Personal Information Protection Commission (PIPC)

South Korea's Personal Information Protection Commission imposed a record-breaking ₩624.68 billion (approximately US$409 million) in combined penalties on e-commerce giant Coupang, the largest personal-data penalty in Korean history, following a breach that exposed the data of approximately 37.55 million people, more than 70% of South Korea's population.

The breach, caused by a former IT employee who retained working system credentials after leaving the company and exfiltrated data undetected between April and November 2025, exposed names, contact details, delivery addresses, and account information for 33.2 million members and a further 4.3 million non-members whose details had been stored as delivery recipients. The PIPC's investigation, prompted in part by parliamentary hearings, also uncovered a separate violation: Coupang's affiliate marketing programme had covertly collected the third-party browsing activity of roughly 11.2 million users without consent, drawing a further ₩201.1 billion penalty. The regulator cited inadequate authentication-key management, absent access controls, interference with the independence of Coupang's data protection officer, and obstruction of the investigation (including deletion of access logs) as aggravating factors. Coupang has announced it will challenge the decision in court.

India / DPDP Act 2023 - Compliance Angle: The Coupang case is the clearest global illustration to date of the financial scale DPDP Act 2023 penalties could reach once the Schedule's revenue-linked ceilings become enforceable: the PIPC calculated its fine as a percentage of Coupang's average annual revenue over the three years preceding the breach, a methodology comparable in spirit to the DPDP Act's own maximum-penalty architecture. The root cause, offboarded staff retaining working access to production systems, is a basic access-control failure. Indian data fiduciaries should treat credential revocation on employee exit as a tested, auditable control, not a checklist item, and should log and monitor all administrative access to systems holding personal data at scale.

Primary Source: Personal Information Protection Commission (Korea) — Enforcement Decision Briefing, 11 June 2026 · **News Coverage:** Bloomberg: South Korea Fines Coupang $409 Million for Large-Scale Data Leak

04. Vodafone España, S.A.U. & Amadeus IT Group, S.A.

€15,450,000 (Combined; Vodafone €1.05M + Amadeus €14.4M)

Spain · Agencia Española de Protección de Datos (AEPD) · *Published in the Boletín Oficial del Estado (BOE)*

Spain's AEPD published two significant GDPR sanctions exceeding €1 million in the national gazette on 17 June 2026, as required under Article 76.4 of the LOPDGDD. Vodafone España was fined €1.05 million across three infringements: two separate €150,000 penalties for processing personal data without a valid legal basis (Article 6.1 GDPR) and a €750,000 penalty, the largest single component, for inadequate technical and organisational security measures under Article 32 GDPR, covering deficiencies in encryption, access control, incident management, and risk assessment.

The same gazette publication carried the AEPD's closure of proceedings against Amadeus IT Group, the global travel-technology provider, following a €14.4 million voluntary payment (a 20% reduction from an original €18 million fine). Amadeus had run an internal pilot between December 2021 and June 2022, combining its own Passenger Name Record (PNR) booking data, including archived records from 2019, with hotel-chain customer data to build a traveller profiling and personalisation product, without informing the millions of affected travellers or establishing a valid legal basis. The AEPD rejected Amadeus's reliance on legitimate interest, finding that travellers had no reasonable expectation their booking data would be repurposed for a new commercial product years later.

India / DPDP Act 2023 - Compliance Angle: Both cases turn on the same principle embedded in DPDP Act 2023 Section 6: consent and notice must be tied to a specific processing purpose, and data collected for one purpose (a telecom subscription, a travel booking) cannot be silently repurposed without fresh notice. The Amadeus case is particularly instructive for Indian B2B technology and platform providers: even where an organisation has no direct relationship with the end data principal, it remains independently accountable for the purposes to which it puts data it receives through a business partner.

Primary Source: AEPD / Boletín Oficial del Estado — Resolución de 17 de junio de 2026 (BOE-A-2026-14010) · **News Coverage:** DataGuidance: Spain, AEPD closes €18M fine against Amadeus after €14.4M voluntary payment

05. Emirates (Airline)

€180,000

Italy · Garante per la Protezione dei Dati Personali, Provvedimento n. 347/2026 · *17 June 2026*

Italy's Garante fined the Dubai-based airline Emirates €180,000 following a complaint from a passenger with reduced mobility, over the airline's handling of health data collected through its MEDIF (Medical Information for Fitness to Travel) questionnaire. The complainant was required to complete the MEDIF form, which collects detailed health information including the treating physician's details and any accompanying carer, despite not falling within the categories of passengers for whom the form is mandatory; assistance was made conditional on completing it regardless.

The Garante confirmed that airlines may lawfully process the health data of passengers with disabilities or reduced mobility without consent where necessary for safe transport and assistance, consulting Italy's civil aviation authority (ENAC) in reaching this conclusion. It nonetheless found two violations: inadequate transparency, since Emirates provided no sufficiently clear notice about MEDIF data processing on its website or through assistance staff, and excessive retention, since health data collected via MEDIF was kept for seven years, a period the Authority found disproportionate to the purpose of organising a single journey. Emirates was ordered to update its

privacy notice, clarify which passenger categories and form sections are genuinely mandatory, and delete data retained beyond a justified period.

India / DPDP Act 2023 - Compliance Angle: Special category data such as health information receives no separate statutory tier under the DPDP Act 2023 as it does under GDPR Article 9, but Sections 5 and 8 still require clear notice and proportionate retention for any personal data, sensitive or not. Indian airlines, healthcare platforms, and insurers collecting health information for legitimate safety or underwriting purposes should audit retention schedules specifically: a lawful basis for collection does not extend indefinitely, and data collected for one journey or policy period should not be retained years beyond its purpose.

Primary Source: Garante per la Protezione dei Dati Personali — Provvedimento n. 347/2026, 17 June 2026 · **News Coverage:** Altalex: Privacy ad alta quota, il Garante sanziona Emirates per i dati sanitari dei passeggeri

06. State of Florida v. TikTok Inc., ByteDance Ltd. et al.

Civil Lawsuit Filed

Florida, United States · Florida Attorney General James Uthmeier, 19th Judicial Circuit, St. Lucie County · *15 June 2026*

Florida Attorney General James Uthmeier filed a civil lawsuit against TikTok and parent company ByteDance, alleging violations of Florida's Online Protections for Minors Act (House Bill 3), which took effect 1 January 2025 and bars children under 14 from holding social media accounts while requiring verifiable parental consent for 14- and 15-year-olds. The complaint alleges TikTok continues to permit underage sign-ups and misrepresents the platform's content ratings.

The complaint alleges TikTok's app-store content descriptions characterise sexual content, drug and alcohol references, profanity, and self-harm material as "infrequent" or "mild" when, according to the state, such content is in fact frequent and appears in graphic detail, including through algorithmic search suggestions. Florida further alleges TikTok's engagement-optimised recommendation system is designed to foster compulsive use among minors and seeks a declaration that the platform constitutes a public nuisance, alongside civil penalties, disgorgement, and injunctive relief. TikTok stated it is engaging with the Attorney General's office and has begun suspending known under-14 accounts in Florida; the company is separately named in lawsuits from more than 25 U.S. state attorneys general over alleged design-related harm to young users.

India / DPDP Act 2023 - Compliance Angle: Florida's complaint targets a gap that also exists under Indian law: age-gating that relies on self-declared birthdates is not, on its own, "verifiable" parental consent within the meaning of DPDP Act 2023 Section 9. The lawsuit's second theme, that platform content-rating disclosures did not match actual user experience, is a transparency failure distinct from the consent failure, and is a useful reminder that notice obligations under Section 5 extend to accurately describing the nature of content and risk a child may encounter, not merely to collection and use of personal data.

Primary Source: Florida Attorney General — Complaint, Office of the Attorney General v. TikTok Inc. et al., 15 June 2026 · **News Coverage:** Washington Examiner: Florida sues TikTok for violating state law restricting minors' access to platform

07. AgID — Agenzia per l'Italia Digitale

€55,000

Italy · Garante per la Protezione dei Dati Personali, Provvedimento n. 419/2026 · *Decided 28 May 2026; published and widely reported from 18 June 2026*

In an unusual instance of one Italian public authority sanctioning another, the Garante fined AgID, the government agency responsible for coordinating Italy's public-sector digital transformation and its national AI regulation role, €55,000 for unlawfully transferring professionals' certified email (PEC) addresses from the long-standing INI-PEC register into the newer National Digital Domiciles Index (INAD) without adequate notice.

The Garante found that AgID moved PEC addresses en masse into INAD, a publicly searchable, unauthenticated register used to deliver legally binding communications from public bodies, without informing affected professionals or giving them an opportunity to select a different digital domicile before publication, in direct violation of AgID's own INAD guidelines. The Authority noted the practical risk: many professionals' PEC inboxes are shared with colleagues or staff, meaning legally significant notices, including penalty notices, could reach an inbox never intended to receive them. The decision was adopted on 28 May 2026 but only became widely known through Italian press coverage from mid-June, once the Garante published the ruling.

India / DPDP Act 2023 - Compliance Angle: The DPDP Act 2023 draws no distinction between government and private-sector data fiduciaries when it comes to core obligations: Section 5 notice requirements and Section 4 purpose-limitation principles apply equally to a government digital-identity system as to a private company. As India expands digital public infrastructure such as the DigiLocker and Account Aggregator ecosystems, this case is a caution that repurposing one government-held identifier (an address originally registered for one legal purpose) for a new, broader use requires the same fresh notice and choice that would be expected of a private controller.

Primary Source: Garante per la Protezione dei Dati Personali — Provvedimento n. 419/2026, 28 May 2026 · **News Coverage:** Agenda Digitale: AgID multata per le PEC in INAD: la sanzione che riguarda la privacy di tutti

08. Council of Europe — ShinyHunters Data Breach

429,000+ Documents Exposed (Confirmed Leak)

Strasbourg, France / 46 Member States · Council of Europe (intergovernmental human-rights body); extortion group ShinyHunters · *Claimed 13–15 June 2026; leak deadline 16 June 2026; data published thereafter*

The extortion group ShinyHunters claimed responsibility for a breach of the Council of Europe, the 46-nation intergovernmental human-rights body, alleging theft of 297GB of data across 429,000 files from the Secretariat, Human Resources Directorate, Parliamentary Assembly, and the European Directorate for the Quality of Medicines and HealthCare. The group set a 16 June 2026 deadline for the Council to make contact, warning it would otherwise leak the data; when no agreement was reached, the group published the archive and has since made it permanently available via mirrors and torrents.

The claimed dataset includes more than 409,000 payslips spanning 2011–2026 for over 10,000 current and former staff, 14,000 CVs, 3,700 personnel files, and records covering bank account

details, tax and social security information, medical records, home addresses, and dates of birth. Security researchers have linked the intrusion to a wider campaign exploiting a zero-day vulnerability (CVE-2026-35273, CVSS 9.8) in Oracle PeopleSoft's Environment Management Hub, which has separately compromised over 100 organisations including the University of Nottingham. The Council of Europe confirmed it is investigating but had not, at the time of reporting, announced a notification plan for affected individuals.

India / DPDP Act 2023 - Compliance Angle: This incident is a direct illustration of why DPDP Act 2023 Section 8(6) breach-notification timelines matter operationally, not just as a compliance formality: an unpatched, actively exploited vulnerability in enterprise HR and payroll software (a category almost every large Indian organisation runs) can expose a decade or more of employee financial and health data before detection. Organisations running PeopleSoft or comparable legacy ERP/HR platforms should confirm patch status against publicly disclosed CVEs immediately and treat HR and payroll systems as high-sensitivity assets requiring the same monitoring rigour as customer-facing systems.

Primary Source: Council of Europe — Statement Confirming Investigation, June 2026 · **News Coverage:** BleepingComputer: Council of Europe investigates ShinyHunters data breach claims

09. KRA Consultancy Ltd

£300,000

United Kingdom · Information Commissioner's Office (ICO) · *23 June 2026*

The ICO fined Manchester-based KRA Consultancy Ltd £300,000 for breaching the Privacy and Electronic Communications Regulations 2003 (PECR) after an investigation into unsolicited direct marketing. KRA sent unsolicited text messages promoting debt-solution services, in some cases using fabricated bailiff threats to pressure recipients into responding.

The ICO issued an enforcement notice alongside the fine, requiring KRA to cease the unlawful marketing practices within 30 days. The case is part of the ICO's ongoing focus on unsolicited electronic marketing under Regulation 22 of PECR, which requires prior consent before sending direct marketing messages to individuals.

India / DPDP Act 2023 - Compliance Angle: While the DPDP Act 2023 does not directly regulate unsolicited marketing in the way PECR does (that falls more within TRAI's telecom regulatory framework in India), the underlying conduct, using fabricated authority or urgency to pressure a data subject into engaging, is directly relevant to Section 6's consent-quality requirements: consent obtained through deceptive framing or manufactured urgency is not "free" consent within the meaning of the Act. Indian financial-services marketers and recovery agents should treat this as a caution against manufactured-urgency messaging generally, not just as a telecom-marketing issue.

Primary Source: Information Commissioner's Office — Enforcement Notice and Monetary Penalty Notice, 23 June 2026 · **News Coverage:** DataGuidance: UK, ICO fines KRA Consultancy Ltd £300,000 for direct marketing violations

10. Elkjøp Nordic AS & Elkjøp AS

NOK 20,000,000 (approx. US$2.14 Million)

Norway · Datatilsynet (Norwegian Data Protection Authority) · *4 June 2026*

Norway's Datatilsynet fined electronics retailer Elkjøp NOK 20 million for processing personal data without a valid legal basis under the GDPR. The decision follows an investigation into how Elkjøp collected and used customer data across its retail and after-sales service operations without establishing adequate consent or an alternative lawful basis for the processing in question.

> **India / DPDP Act 2023 - Compliance Angle:** Retail and consumer-electronics businesses in India that collect customer data at point of sale, for warranty registration, after-sales service, or loyalty programmes, should treat this as a direct parallel: DPDP Act 2023 Section 6 requires a valid basis for each processing purpose, and a single blanket consent captured at checkout will rarely cover every downstream use (service reminders, marketing, cross-selling) a retailer may want to make of that data.

Primary Source: Datatilsynet — Enforcement Decision, 4 June 2026 · **News Coverage:** DataGuidance: Norway, Datatilsynet fines Elkjøp NOK 20M for processing personal data without valid consent

11. Bithumb Korea Co., Ltd.

₩210,000,000 (approx. US$136,000)

South Korea · Personal Information Protection Commission (PIPC), 12th Plenary Session · *24 June 2026*

South Korea's PIPC fined cryptocurrency exchange Bithumb ₩210 million and issued a corrective order after finding the company transferred users' personal information overseas without proper consent while sharing USDT order-book data with a foreign exchange between September and November 2025. Although Bithumb had told users their data would go to the Stellar exchange, investigators found it was actually transferred to a platform operated by BingX, a different entity entirely.

The PIPC separately found that Bithumb shared customer names, dates of birth, and wallet addresses with 13 other overseas exchanges during asset transfers without obtaining complete consent. The decision was issued alongside new PIPC guidelines for blockchain companies, which recommend keeping personally identifiable information off public ledgers and verifying the actual destination of any cross-border data transfer rather than relying on partner representations.

> **India / DPDP Act 2023 - Compliance Angle:** The core failure, telling users data would go to one recipient while it was actually processed by an unrelated third party, is a transparency violation directly analogous to DPDP Act 2023 Section 5's notice requirements. Indian crypto exchanges and fintech platforms using overseas liquidity partners, cloud infrastructure, or compliance vendors should independently verify the actual data flow end-to-end rather than relying on a counterparty's stated destination.

Primary Source: Personal Information Protection Commission (Korea) — 12th Plenary Session Decision, 24 June 2026 · **News Coverage:** The Korea Herald: Privacy watchdog fines Bithumb W210m for violating overseas data transfer rules

12. Roku, Inc.

$25,000,000 (Committed Investment; No Civil Fine)

Florida, United States · Florida Attorney General James Uthmeier · *26 June 2026*

Florida's Attorney General announced a negotiated resolution with Roku, Inc. of the enforcement action filed under the Florida Digital Bill of Rights (FDBR), which had alleged Roku improperly collected, processed, and in some cases sold children's personal information, including device identifiers, IP addresses, and precise geolocation data, without proper consent or effective age-assurance measures. The resolution includes no finding of wrongdoing and no civil fine.

Under the agreement, Roku committed to invest an estimated $25 million in engineering resources to enhance child-protection features, giving parents greater control over their children's streaming experience, with full nationwide deployment expected within twelve months. The case was the first enforcement action brought under the FDBR, which took effect in July 2024 and permits civil penalties of up to $150,000 per violation involving a known child.

India / DPDP Act 2023 - Compliance Angle: Roku's alleged conduct, using cartoon screensavers and clearly child-directed content categories while denying "actual knowledge" that children were using the platform, mirrors the kind of willful disregard argument that Indian regulators are likely to test under DPDP Act 2023 Section 9. Platforms cannot market features to children and simultaneously claim ignorance of a child user base; Indian streaming, gaming, and connected-device platforms should treat demonstrable engagement with child-directed content categories as actual or constructive knowledge triggering verifiable parental consent obligations.

Primary Source: Florida Attorney General — Press Release, 26 June 2026 · **News Coverage:** DataGuidance: Florida, AG announces resolution with Roku over digital privacy enforcement action

13. Schibsted (Aftenposten, VG, Bergens Tidende)

Formal GDPR Complaint Filed (Fine Requested)

Norway · Norwegian Consumer Council (Forbrukerrådet) & noyb, filed with Datatilsynet · *3 June 2026*

The Norwegian Consumer Council and the privacy advocacy group noyb filed a joint complaint with Datatilsynet against Nordic media group Schibsted over its "pay or okay" model, which requires readers of Aftenposten, VG, and Bergens Tidende to either consent to personalised advertising tracking or pay a monthly subscription fee to avoid it. The complaint asks Datatilsynet to declare the practice unlawful and to impose a fine, arguing it violates Article 7 GDPR's requirement that consent be freely given.

The complaint follows Datatilsynet's own critical public statement on 30 April 2026 regarding Schibsted's 39-krone monthly privacy fee, and comes after Sweden's data protection authority received more than 56 individual complaints when Schibsted's Swedish subsidiary introduced the same model in March 2026. noyb argues that because personalised tracking is not necessary to deliver a news article, conditioning access on payment for its absence converts consent into a financial transaction rather than a genuine free choice.

India / DPDP Act 2023 - Compliance Angle: India's DPDP Act 2023 does not contain an equivalent express "freely given" consent test tied to a pay-or-consent model, but Section 6's requirement that consent be "free, specific, informed, unconditional and unambiguous" raises the same underlying

question. Indian digital publishers experimenting with subscription-versus-tracking models should document a genuine, low-friction alternative that does not financially penalise a reader for declining tracking-based consent.

Primary Source: noyb / Norwegian Consumer Council — Complaint under Article 77(1) GDPR, 3 June 2026 · **News Coverage:** DataGuidance: Norway, NCC and NOYB file complaint against Schibsted over 'pay or okay' model

14. Altex România S.R.L.

RON 52,086 (approx. €10,000)

Romania · Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) · *18 June 2026*

Romania's data protection authority fined electronics retailer Altex România €10,000, its third separate GDPR sanction within roughly eighteen months, after a technical vulnerability in the company's mobile app account-validation process allowed unauthorised access to a third party's personal data, including name, invoices, and delivery address. The ANSPDCP found violations of Article 32(1)(b) and (d) and Article 32(2) for inadequate technical and organisational security measures, and of Articles 33(1) and 34(1) for failing to notify the authority or the affected individual of the breach.

India / DPDP Act 2023 - Compliance Angle: Repeated security-related fines against the same retailer within a short period, following two earlier 2024 sanctions for similar app vulnerabilities, illustrate a pattern regulators treat as an aggravating factor: remediation after one incident does not exempt an organisation from liability for a structurally similar failure later. Indian e-commerce platforms should treat each security incident as a trigger to review the entire application stack for the same class of vulnerability, not just the specific instance reported.

Primary Source: ANSPDCP — Press Release, 18 June 2026 · **News Coverage:** JURIDICE.ro: ANSPDCP sancționează Altex

SECTION II — APRIL–MAY 2026 ENFORCEMENT: ESSENTIAL CONTEXT FOR JUNE

Five major decisions finalised shortly before June 2026 shaped the regulatory environment in which June's actions were issued.

C1. Poste Italiane S.p.A. & Postepay S.p.A. — Italy | Garante

€12,501,000 (Combined)

Italy · Garante per la Protezione dei Dati Personali · *Provvedimento n. 237/2026, 17 April 2026 (published 20 April 2026)*

The Garante fined Poste Italiane €6.624 million and its subsidiary Postepay €5.877 million after finding that the companies' BancoPosta and Postepay mobile apps made continued use

conditional on users authorising broad monitoring of installed and running applications on their devices, ostensibly for anti-fraud purposes. The Authority found this device-level surveillance excessively invasive relative to its stated purpose, alongside inadequate notice, no DPIA, and irregular processor designation. Poste Italiane has announced it will appeal.

> **India / DPDP Act 2023 - Compliance Angle:** A legitimate security purpose, such as fraud prevention, does not automatically justify the most invasive available technical measure. DPDP Act 2023's proportionality expectations under Section 8(5) require Indian banking and fintech apps to select security controls calibrated to genuine risk, not default to maximal device access because a payments-security regulation references anti-fraud measures in general terms.

Primary Source: Garante per la Protezione dei Dati Personali — Provvedimento n. 237/2026, 17 April 2026 · **News Coverage:** Il Sole 24 Ore: Privacy fine of €12.5 million for Italian postal regulator

C2. IQVIA Operations France — France | CNIL

€5,000,000

France · Commission Nationale de l'Informatique et des Libertés (CNIL) · *Délibération SAN-2026-008, 26 May 2026*

The CNIL fined IQVIA's French subsidiary €5 million over its management of two CNIL-authorised health-data warehouses used for pharmaceutical research, covering tens of millions of patients. Investigators found no regular review of connection logs, no multi-factor authentication on one warehouse, inaccurate patient notices, and a pharmacy-management software design that transmitted patient data even where a patient had refused. IQVIA argued the data were anonymous following a September 2025 CJEU ruling; the CNIL held the data remained merely pseudonymous and re-identifiable, and therefore squarely within GDPR's scope.

> **India / DPDP Act 2023 - Compliance Angle:** The pseudonymisation-versus-anonymisation distinction matters directly under the DPDP Act 2023: data that can be re-identified by reasonable means, even after a masking or tokenisation process, remains "personal data" under Section 2(t) and stays fully within the Act's scope. Indian health-data platforms and research bodies relying on de-identification as a basis for reduced compliance obligations should test that assumption against a realistic re-identification risk analysis, not an internal assertion of anonymity.

Primary Source: CNIL — Délibération SAN-2026-008, 26 May 2026 · **News Coverage:** CNIL: Health data — fine of 5 million euros against IQVIA

C3. Amadeus IT Group, S.A. (Original Decision) — Spain | AEPD

€18,000,000 (Reduced to €14.4M)

Spain · Agencia Española de Protección de Datos (AEPD) · *26 May 2026 (publication via BOE followed on 17 June 2026 — see Item 04 above)*

The AEPD's original decision against Amadeus IT Group, closed following a €14.4 million voluntary payment, found two very serious GDPR infringements: a €9 million penalty under Article 14 for failing to specifically inform travellers that their booking data was being repurposed for a profiling pilot, and a further €9 million under Article 6 for lacking any valid lawful basis for that repurposing.

The case is covered in full in Item 04, reflecting its formal publication in Spain's official gazette during June.

> **India / DPDP Act 2023 - Compliance Angle:** See Item 04 above for the full compliance analysis applicable to this decision.

Primary Source: AEPD — Enforcement Decision, closed 26 May 2026 · **News Coverage:** PhocusWire: Spain fines Amadeus €14.4M over traveler profiling pilot

C4. Fortum Energia S.A. & Pika Sp. z o.o. — Poland | UODO / Court

PLN ~5,250,000 (Combined, Upheld on Appeal)

Poland · Provincial Administrative Court in Warsaw, upholding UODO's decision · *20 May 2026*

Poland's Provincial Administrative Court in Warsaw upheld the data protection authority's fines against energy retailer Fortum (approximately PLN 5 million) and its IT processor Pika (over PLN 250,000) over a data breach affecting more than 90,000 individuals. During system modernisation work, Pika created an additional database populated with live Fortum customer data and made it accessible incorrectly; the court confirmed that a controller cannot shift full responsibility for data security onto its processor, even where the processor's own error triggered the exposure.

> **India / DPDP Act 2023 - Compliance Angle:** DPDP Act 2023 places compliance obligations primarily on the data fiduciary, but this case is a reminder that outsourcing technical work to a data processor does not transfer accountability. Indian data fiduciaries engaging IT modernisation or migration vendors should contractually require, and periodically audit, that live production data is never used in test or development environments without equivalent safeguards.

Primary Source: Provincial Administrative Court, Warsaw — Judgment, 20 May 2026 · **News Coverage:** GRC Report: Poland's Supreme Administrative Court Revives GDPR Fines Against Fortum & Pika

C5. Manage My Health Ltd. & Health New Zealand — New Zealand | OPC

Compliance Notices (No Monetary Penalty Under NZ Law)

New Zealand · Office of the Privacy Commissioner (OPC), Phase 1 Inquiry Findings · *27 May 2026*

New Zealand's Privacy Commissioner found that patient health portal Manage My Health (MMH) and Health New Zealand both breached Rule 5 of the Health Information Privacy Code following a December 2025 cyberattack that exposed the sensitive health information of 99,416 patients, 91% of them in Northland, disproportionately affecting Māori patients. Stolen credentials were used to access and copy documents from thousands of patient accounts; Health NZ's own project team lacked specialist privacy and security personnel and relied on MMH's self-reported assurances rather than independent verification.

> **India / DPDP Act 2023 - Compliance Angle:** The finding that a government health body's project team lacked specialist privacy and security personnel, and relied on a vendor's own assurances instead of independent verification, is directly relevant to India's expanding digital health infrastructure (ABDM, health data exchanges). Indian public and private health bodies contracting third-party patient portals

must build independent security verification into the contracting process itself, not treat the vendor's own compliance claims as sufficient due diligence.

Primary Source: Office of the Privacy Commissioner (New Zealand) — Executive Summary, Phase 1 Inquiry, 27 May 2026 · **News Coverage:** DataGuidance: New Zealand, OPC finds MMH and Health NZ breach Privacy Act

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 now under eleven 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 JUNE 2026 ENFORCEMENT

1. Treat administrative access revocation as a tested control, not a checklist item

Coupang's $409M penalty traced back to a departed employee who retained working system credentials for months. Every organisation handling personal data at scale must verify that offboarding actually revokes access on day one, log all administrative access to systems holding personal data, and periodically audit for orphaned or stale credentials.

2. Re-examine every instance of repurposed data against its original notice

The Vodafone and Amadeus decisions both turn on data collected for one purpose (a subscription, a travel booking) being reused for another (marketing, profiling) without fresh, specific notice. Organisations must map every secondary use of previously collected data and confirm a valid, documented legal basis exists for each one.

3. Do not rely on self-declared age as verifiable parental consent

Florida's suit against TikTok reinforces a global regulatory consensus, also reflected in the ICO's Reddit decision earlier in 2026, that unverified self-declaration of age does not satisfy children's-data consent obligations. Platforms likely to be accessed by minors need effective, auditable age-assurance mechanisms, not a checkbox.

4. Patch enterprise HR, payroll, and ERP systems as a matter of urgency

The Council of Europe breach traces to an actively exploited zero-day in Oracle PeopleSoft that has already compromised over 100 organisations. HR and payroll platforms hold years of combined financial, health, and identity data and deserve the same patch-management discipline as customer-facing systems.

5. Set retention limits by purpose, not by convenience

Emirates retained sensitive health data for seven years against a stated purpose of organising a single journey. Every category of sensitive personal data an organisation holds should have a documented retention period tied to why it was collected, with a defined deletion or anonymisation trigger.

6. Public-sector and government-linked bodies are not exempt from core obligations

The Garante's fine against Italy's own digital agency, AgID, confirms that government bodies operating identity, communication, or registry infrastructure face the same notice and purpose-limitation obligations as private companies. Indian public digital infrastructure programmes should build in the same consent and notice discipline expected of private data fiduciaries.

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