Desk "Assistenza e Tutela della Proprietà Intellettuale e Ostacoli al Commercio"

ICE New Delhi

Articolo di approfondimento – Marzo 2026

Il nuovo quadro normativo indiano in materia di protezione dei dati personali: inquadramento sistematico e profili operativi

Il sistema di protezione dei dati personali in India ha conosciuto una significativa evoluzione con l'adozione della disciplina attuativa del Digital Personal Data Protection Act, 2023 (DPDP Act). In particolare, il Ministero dell'Elettronica e delle Tecnologie dell'Informazione (MeitY), con notifica del 14 novembre 2025, ha emanato le Digital Personal Data Protection Rules, 2025 (DPDP Rules), completando il quadro normativo e rendendo pienamente operativo il regime di tutela dei dati personali.

Il DPDP Act, letto congiuntamente alle DPDP Rules, costituisce oggi il principale riferimento normativo in materia di trattamento dei dati personali digitali in India. Esso introduce un sistema organico volto a garantire un utilizzo responsabile dei dati personali, imponendo obblighi puntuali in capo ai soggetti che effettuano trattamenti e prevedendo meccanismi di tutela contro utilizzi indebiti e accessi non autorizzati. L'ambito di applicazione della disciplina ricomprende tutte le attività di trattamento connesse all'offerta di beni o servizi, inclusi i dati originariamente raccolti in forma non digitale e successivamente digitalizzati .

Sotto il profilo soggettivo, il DPDP Act individua tre figure centrali: il *Data Principal*, ossia la persona fisica cui i dati si riferiscono, titolare di specifici diritti tra cui accesso, rettifica e cancellazione; il *Data Fiduciary*, vale a dire il soggetto che determina le finalità e i mezzi

del trattamento ed è responsabile della sua liceità e sicurezza; e il *Data Processor*, che tratta i dati per conto del *Data Fiduciary*. La distinzione tra tali figure non è meramente classificatoria, ma riflette una precisa allocazione delle responsabilità lungo la catena del trattamento.

Dal punto di vista sistematico, il DPDP Act definisce il quadro normativo generale, mentre le DPDP Rules ne precisano i profili operativi, segnando il passaggio da un modello ancora in parte programmatico a un sistema pienamente in vigore e con carattere cogente.

Un primo ambito di rilievo riguarda il regime del consenso e dell'informativa. Il *Data Fiduciary* è tenuto a fornire, prima della raccolta dei dati, un'informativa chiara, autonoma e comprensibile, nella quale siano specificate la natura dei dati trattati e le finalità del trattamento. Particolare enfasi è posta sulla necessità di garantire che la revoca del consenso sia agevole quanto la sua prestazione. Nel caso di dati relativi a minori, è inoltre richiesto il consenso verificabile del genitore o del tutore legale.

Il quadro normativo consente il trasferimento transfrontaliero dei dati personali, seppur subordinato alle condizioni che saranno stabilite dal Governo, e impone l'adozione di adeguate misure di sicurezza, tra cui sistemi di cifratura, controlli sugli accessi e verifiche periodiche. In tale contesto, assume rilievo la formalizzazione contrattuale delle misure di protezione dei dati nei rapporti tra *Data Fiduciary* e *Data Processor*, a conferma della crescente centralità della governance contrattuale del dato.

Le DPDP Rules introducono inoltre la figura del *Consent Manager*, soggetto deputato a consentire agli interessati di prestare, gestire e revocare il consenso attraverso piattaforme digitali sicure e accessibili. Tali soggetti sono tenuti a rispettare stringenti requisiti organizzativi, tra cui l'assenza di conflitti di interesse, il divieto di esternalizzazione delle funzioni essenziali e l'obbligo di conservazione della documentazione per un periodo di sette anni. Possono assumere tale ruolo esclusivamente società costituite in India con un patrimonio netto minimo di INR 2 crore (circa 200.000 euro).

Particolare attenzione è riservata alle misure di sicurezza e alla gestione degli incidenti. I soggetti coinvolti nel trattamento sono tenuti ad adottare misure tecniche e organizzative adeguate, tra cui la protezione dei dati mediante tecniche di cifratura o mascheramento, sistemi di rilevazione degli incidenti e piani di continuità operativa. In caso di violazione dei dati personali, il *Data Fiduciary* è tenuto a notificare l'evento al Data Protection Board entro 72 ore, fornendo informazioni dettagliate su cause, impatti e misure adottate, nonché a informare tempestivamente gli interessati. Analoghi obblighi di segnalazione gravano sul *Data Processor* nei confronti del *Data Fiduciary*.

Il sistema riconosce inoltre agli interessati un insieme articolato di diritti, tra cui il diritto di accesso, aggiornamento, rettifica e cancellazione dei dati, nonché la possibilità di delegare l'esercizio di tali diritti a soggetti terzi. I *Data Fiduciaries* sono tenuti a rispondere alle richieste entro 90 giorni, assicurando un'effettiva tutela dei diritti riconosciuti.

Con riferimento alla conservazione dei dati, la disciplina impone la cancellazione dei dati personali una volta esaurita la finalità del trattamento, salvo obblighi di legge contrari. Tuttavia, per alcune categorie di piattaforme di grandi dimensioni (tra cui e-commerce, social media e piattaforme di gaming con oltre 20 milioni di utenti), è previsto un obbligo di conservazione per un periodo di tre anni, accompagnato dall'obbligo di informare gli interessati almeno 48 ore prima della cancellazione. I registri delle attività di trattamento devono essere conservati per almeno un anno.

Il legislatore introduce, inoltre, la categoria dei *Significant Data Fiduciaries*, individuati sulla base di criteri quali volume e sensibilità dei dati trattati. A tali soggetti si applicano obblighi rafforzati, tra cui la conduzione di valutazioni d'impatto (*Data Protection Impact Assessment*), la sottoposizione ad audit indipendenti e la nomina di un responsabile della protezione dei dati (*Data Protection Officer*).

Sotto il profilo temporale, l'attuazione delle DPDP Rules è articolata secondo un approccio graduale. In una prima fase, è stata istituita l'architettura istituzionale, inclusa la creazione del Data Protection Board. Entro 12 mesi è previsto l'avvio del regime applicabile ai *Consent Managers*, mentre entro 18 mesi il sistema diverrà pienamente operativo, con conseguente applicazione delle sanzioni in caso di inadempimento .

Il regime sanzionatorio previsto dal DPDP Act si caratterizza per un approccio proporzionale, con sanzioni differenziate in funzione della gravità della violazione. In particolare, le violazioni relative all'adozione di misure di sicurezza possono essere sanzionate fino a INR 250 crore (circa 250.000 euro), mentre la mancata notifica di una violazione può comportare sanzioni fino a INR 200 crore (circa 200.000 euro). Ulteriori violazioni, tra cui quelle relative agli obblighi dei *Significant Data Fiduciaries*, possono comportare sanzioni fino a INR 150 crore (circa 150.000 euro).

In termini sistematici, il nuovo quadro normativo segna il passaggio verso un modello di regolazione fondato sulla responsabilizzazione dei soggetti che trattano dati personali, nel quale l'adempimento non si esaurisce in obblighi formali, ma richiede l'adozione di un sistema organizzativo e documentale idoneo a garantire, in concreto, la conformità alla disciplina. Per gli operatori economici, e in particolare per le imprese straniere attive sul mercato indiano, ciò comporta la necessità di strutturare processi interni, flussi

contrattuali e presidi di sicurezza in linea con i requisiti normativi, in un'ottica di compliance sostanziale e continuativa.

Il Desk resta a disposizione per approfondimenti specifici.

***

Il presente articolo è frutto della libera interpretazione e sintesi delle fonti ivi menzionate da parte dell'Avv. Riccardo Verzella, in qualità di Avvocato responsabile del Desk "Assistenza e Tutela della Proprietà Intellettuale e Ostacoli al Commercio" costituito presso l'Agenzia ICE di New Delhi unitamente agli altri professionisti dello Studio D'Andrea & Partners Legal Counsel e non costituisce in ogni caso un parere legale sulle questioni trattate, né può dar luogo a legittimi affidamenti o fondare iniziative di natura legale. Per eventuali richieste di chiarimenti, vi invitiamo a fare riferimento all'indirizzo e-mail ipr.newdelhi@ice.it

***

The Indian Data Protection Framework: Systematic Overview and Practical Implications

India's data protection regime has undergone a significant evolution with the adoption of the implementing framework of the Digital Personal Data Protection Act, 2023 (DPDP Act). In particular, the Ministry of Electronics and Information Technology (MeitY), through its notification dated 14 November 2025, issued the Digital Personal Data Protection Rules, 2025 (DPDP Rules), thereby completing the regulatory framework and rendering the system fully operational.

The DPDP Act, read together with the DPDP Rules, now constitutes the primary legal framework governing the processing of digital personal data in India. It establishes a structured regime aimed at ensuring the responsible use of personal data, imposing clear obligations on entities processing such data and providing safeguards against misuse and unauthorized access. The framework applies to all processing activities connected with the offering of goods or services, including personal data initially collected in non-digital form and subsequently digitised .

From a structural standpoint, the DPDP Act identifies three key actors: the Data Principal, namely the individual to whom the personal data relates; the Data Fiduciary, which determines the purposes and means of processing and bears primary responsibility for compliance; and the Data Processor, which processes data on behalf of the Data Fiduciary. This classification reflects a clear allocation of responsibilities within the data processing chain.

While the DPDP Act establishes the statutory framework, the DPDP Rules define its operational contours, marking the transition from a policy-oriented approach to a fully enforceable compliance regime.

A central element of the framework concerns notice and consent. Data Fiduciaries are required to provide clear and standalone notices prior to data collection, specifying the nature of the data and the purposes of processing. Particular emphasis is placed on ensuring that the withdrawal of consent is as easy as its provision. In the case of children's data, verifiable parental or guardian consent is required.

The framework allows cross-border transfers of personal data, subject to conditions to be specified by the Government, and mandates the implementation of appropriate security safeguards, including encryption, access control mechanisms, and periodic audits. In this respect, contractual arrangements between Data Fiduciaries and Data Processors play a key role in ensuring compliance.

The DPDP Rules also introduce the figure of the Consent Manager, an entity responsible for enabling Data Principals to provide, manage, and withdraw consent through secure digital platforms. Such entities are subject to strict requirements, including independence, prohibition of outsourcing core functions, and record retention obligations for a period of seven years. Only companies incorporated in India with a minimum net worth of INR 2 crore may act as Consent Managers .

Significant emphasis is placed on security safeguards and incident management. Data Fiduciaries and Data Processors must implement adequate technical and organisational measures, including data protection techniques, incident detection systems, and business continuity plans. In the event of a personal data breach, the Data Fiduciary is required to notify the Data Protection Board within 72 hours and inform affected individuals without undue delay. Data Processors must, in turn, promptly notify the Data Fiduciary.

The framework further grants Data Principals a comprehensive set of rights, including the right to access, correct, update, and erase personal data, as well as the possibility to authorise third parties to exercise such rights. Data Fiduciaries must respond to such requests within 90 days.

With regard to data retention, personal data must be erased once the purpose of processing has been fulfilled, unless retention is required by law. However, certain large platforms (including e-commerce, social media intermediaries, and gaming platforms exceeding 20 million users) are required to retain data for three years and notify individuals 48 hours prior to deletion. Processing logs must be retained for at least one year.

The Act also introduces the category of Significant Data Fiduciaries, which are subject to enhanced compliance obligations, including the conduct of Data Protection Impact Assessments, independent audits, and the appointment of a Data Protection Officer.

The implementation of the DPDP Rules follows a phased approach. Initially, institutional mechanisms such as the Data Protection Board have been established. Within 12 months, the regulatory regime for Consent Managers will become operational, while within 18 months the framework will be fully enforceable, with penalties applicable in case of non-compliance .

The penalty regime under the DPDP Act is structured on a proportional basis, with sanctions varying according to the nature and severity of the breach. Violations relating to security safeguards may attract penalties of up to INR 250 crore, while failure to report a breach may lead to penalties of up to INR 200 crore. Additional violations, including those concerning Significant Data Fiduciaries, may result in penalties of up to INR 150 crore .

From a systematic perspective, the new framework reflects a shift towards an accountability-based model, where compliance is not limited to formal requirements but requires the adoption of robust organisational and governance structures capable of ensuring substantive adherence to the law. For businesses operating in India, particularly foreign entities, this entails the need to implement structured compliance frameworks, contractual safeguards, and internal processes aligned with the regulatory requirements.

The Desk remains available for further analysis and assistance.

***