How will the 'cookies' crumble under India's new data protection law?

WHAT'S IN A 'COOKIE'?

When a user visits a website, the website stores a small text file in the user's browser. If the user visits that website again using the same browser, the browser automatically sends back this text file, commonly known as a 'cookie' to the website, so that the website can remember the user's preferences, keep the user logged-in, or even restore a previous browsing session. A 'cookie' can be considered as a 'memory note'- to illustrate, the first time a visitor goes to a library (the 'website'), the visitor would provide her personal details (name, literary preferences etc.) to the library and in return receive a customized library card (the 'cookie'). On the visitor's next visit, the library (the 'website') would simply look at the library card (the 'cookie') and 'remember' the visitor's preferences, without needing to ask again.

'Cookies' can be categorized broadly as essential/ strictly necessary 'cookies', performance/ analytics 'cookies', functionality 'cookies', targeting/ advertising 'cookies', social media 'cookies', security 'cookies'. Broadly, depending on who generates the 'cookie' and whether it works only on one or several websites - these may be *first party 'cookies'* (if a user visits website 'A', the website may generate and set a functionality cookie which stores specific user preferences for that website only) or *third party 'cookies'* (if a user visits website 'B' which also displays third party advertisements, an advertiser or tracking network may generate and deploy a 'cookie' to the user's browser. This 'cookie' would track the user's browsing activity across websites, generating a unique user profile that is used for targeted advertising).

Depending on the type of 'cookies', these can either be 'signposts' for personal data or can themselves be generated using a user's personal data. Crucial for both website performance and targeted advertising, 'cookies' sit at the crossroads of a business-need to tap user data for providing relevant and targeted services (including marketing efforts) and the duty to protect user privacy.

IMPLEMENTATION OF THE DPDP ACT

With the phased rollout of India's Digital Personal Data Protection Act, 2023 (**DPDP Act**) and the accompanying Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) in November 2025, India now has a comprehensive framework for the protection of 'digital personal data'[1]. The DPDP Act requires entities to provide notice and obtain consent for processing[2] any personal data (whether in a digital form or digitized subsequently). The DPDP Act places a host of other critical

[1] Section 2(n) of the DPDP Act defines '***digital personal data***' as personal data in digital form. Section 2(t) defines '***personal data***' as any data about an individual who is identifiable by or in relation to such data.

[2] Section 2(x) of the DPDP Act defines '***processing***' as wholly or partly automated operation or set of operations performed on digital personal data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

© ECONOMIC LAWS PRACTICE 2025

obligations on data fiduciaries[3] in relation to their processing activities. Data fiduciaries may also engage other entities known as 'data processors' for processing personal data on their behalf, however, the consequences of any non-compliances under the DPDP Act would be borne only by the data fiduciary.

TREATMENT OF 'COOKIES' UNDER INDIA'S DATA PROTECTION LAW

The new data protection framework under the DPDP Act along with the DPDP Rules will have wide-ranging implications on how digital personal data is processed. In such a scenario, the use and deployment of 'cookies' may raise issues if such 'cookies' are used to access and collect personal data without obtaining clear consent. The use and deployment of 'cookies' may squarely fall under the scope of the DPDP Act, as follows:

- ***'Cookies' as 'personal data' of website users.*** A first party 'cookie' that is stored and then returned from a user's browser to a website, allows that website to 'remember' the user's preferences and the user is identifiable by such a 'cookie'. This also holds true for third-party cookies such as advertiser 'cookies' - these 'cookies' create a unique ID on a user's browser and each time a user visits a website that uses the same advertisers network, over time, the unique ID becomes linked to the user's profile (interests, browsing preferences etc.) and so, a user is identifiable even through such 'cookies'.

  Simply stated, under the DPDP Act, a 'cookie' could qualify as 'digital personal data' because a user can be identified in relation to it and a user would be the 'data principal' in relation to the 'cookie'.

- ***Cookie-setters as 'data fiduciaries'.*** An entity that sets (or causes to set) a 'cookie' could qualify as a 'data fiduciary' under the DPDP Act, since such an entity determines the purpose for which the 'cookie' is being set (which may include re-marketing, analytics, ad-tracking etc.) and the means of processing a user's personal data through such 'cookies'.

WHAT SHOULD DATA FIDUCIARIES KEEP IN MIND?

Once the DPDP Act is fully in force[4], every data fiduciary would be required to mandatorily obtain prior user consent and provide notice before even collecting digital personal data, except in cases where personal data is processed for 'legitimate uses'[5]. Under this new regime, cookie-setting entities will need to mandatorily request consent[6] before deploying 'cookies' along with a notice clearly specifying the categories of personal data and the specified purposes for processing such personal data[7] and the request for consent and notice must meet the requirements stipulated under the DPDP Act. May 2027 onwards, other extensive obligations under the DPDP Act would also be applicable to cookie-setting entities - including, maintaining accurate personal data[8], cessation of processing personal data[9], erasure of personal data if consent has been withdrawn or the specified purpose has been served[10], and data breach redressal[11].

[3] Section 2(i) defines a '***data fiduciary***' as a person who alone or in conjunction with any other person determines the purpose and means of processing personal data.

[4] The implementation timelines for the DPDP Act have been set out through Notification G.S.R. 843(E). dated November 13, 2025.
[5] Section 4(1)(b) of the DPDP Act provides for processing of personal data, without obtaining consent, for certain legitimate uses. Section 7 of the DPDP Act sets out '***legitimate uses***', which include, to comply with a legal obligation to disclose such data, to comply with a judgment of a court, to respond in a medical emergency, etc.
[6] Section 6 of the DPDP Act requires consent to be obtained from a data principal, for processing personal data, for the purpose specified in a notice.
[7] Section 5 of the DPDP Act, read along with Rule 3(b) of the DPDP Rules, requires a data fiduciary to provide a notice to a data principal, setting out, among others, an itemized description of personal data to be processed, the specified purpose(s), and a specific description of goods and services
[8] Section 12(2) of the DPDP Act obligates data fiduciaries to correct and update personal data, following a request from a data principal.
[9] Section 6(6) of the DPDP Act requires a data fiduciary to stop processing a data principal's personal data, within a reasonable period of time, if a data principal withdraws its consent, unless the data fiduciary is required to continue processing under the DPDP Act or any other applicable law.
[10] Section 8(7)(a) of the DPDP Act requires a data fiduciary to erase personal data upon withdrawal of consent by a data principal or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier, unless the data fiduciary is required to retain the data in compliance with applicable law.
[11] The DPDP Act requires a data fiduciary to implement minimum security safeguards to protect personal data and in case of a breach, comply with obligations including notifying data principals and the Data Protection Board of India.

© ECONOMIC LAWS PRACTICE 2025

Ahead of the May 2027 timeline, cookie-setting entities must take necessary steps to align their cookie-related practices with the new statutory framework for data protection. Certain recommended actions that would be a step in the right direction include:

- ***Implementing 'cookie' consent banners.*** As on December 2024, of the top 50 most visited websites in India, only 6% implemented 'cookie' consent banners.[12] As a first step, on a user's first visit, a 'cookie' consent or notice banner must be clearly displayed.
- ***Re-designing 'cookie' consent banners.*** The 'cookie' consent or notice banner must be user-friendly, clearly setting out the types of 'cookies' that may be set and deployed along with clear and easily understandable descriptions of the 'cookies'. The banner must provide granular opt-ins, i.e., users must be able to select specific 'cookies' and not merely a blanket 'accept all' option.
- ***Re-framing 'cookie' policies.*** Clear and comprehensive policies covering use of 'cookies' must include mechanism for consent withdrawal, duration of 'cookies', purpose of deployment of the 'cookies', specifications, details of 'cookie' preference dashboards to allow users to modify preferences etc. The cookie-related policies should preferably be linked within the 'cookie' consent or notice banner.
- ***Consent logs and audits.*** Detailed and updated logs for consent provided by users for deployment of 'cookies' should be maintained, capturing details of consent and regular audits must be undertaken.

WAY FORWARD

Undoubtedly, 'cookies' are central to deliver seamless user experience and tailored advertisements. With the DPDP Act putting a mandatory 'consent' framework for processing digital personal data protection at the forefront, 'cookies' which are linked to a user's personal data, can no longer be used to harvest user information without notice and consent. Cookie-setting entities must carefully evaluate and assess their 'cookie' practices and prepare for full compliance under the DPDP Act. Compliant practices and policies will not only protect users but also instill user trust in the privacy-first approach of such organizations.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -ravisekharnair@elp-in.com

Abhay Joshi, Partner – Email - abhayjoshi@elp-in.com

Aayushi Sharma, Principal Associate – Email - aayushisharma@elp-in.com

Disclaimer: *The information provided in this update is intended for informational purposes only and does not constitute legal opinion or advice.*

[12] *Navigating Cookies: Recalibrating your cookie strategy in light of the DPDPA*, available at: https://www.ascionline.in/wp-content/uploads/2025/01/Navigating-Cookies-Whitepaper.pdf (last accessed on December 2, 2025).