PRIVACY POLICIES IN DPDP ERA: MORE THAN A WEBSITE FORMALITY

Almost every website has a privacy policy. Few visitors read it, and organisations often give it little attention beyond ensuring the link exists. Sometimes, a generic policy comes with the website-building package, without legal review or anyone checking whether it reflects actual data practices.

India already has privacy-policy requirements under the SPDI Rules, 2011, the Intermediary Rules, 2021, and sectoral regulations. The RBI's Digital Lending Directions, 2025, for example, require publicly available policies and disclosure of third parties permitted to collect personal information. The SPDI framework covers collection, use, disclosure and security practices.

The Digital Personal Data Protection Act, 2023 and its Rules ('**DPDP framework**') shift attention towards notices, consent and accountability, without expressly mandating a document called a 'privacy policy'. This makes it worth reconsidering what that document can achieve.

A Data Principal may read a consent notice and still want to understand how her information moves through the organisation. The policy can provide that fuller explanation. The notice must remain independently understandable, with itemised personal data and specified purposes; the policy can add context, examples and detail, without substituting for the notice or expanding consent.

That starts with connecting the data collected to its uses. Why is a telephone number needed? Is location information used for delivery, analytics or both? Answering these questions also forces the organisation to examine whether it understands its own data flows. A policy that cannot be written clearly may reveal practices that have not been thought through clearly.

The same approach should extend to security. The SPDI Rules recognise IS/ISO/IEC 27001; DPDP framework specifies safeguards covering encryption or comparable protections, access controls, monitoring, backups, retention of logs and data, processor contracts, and technical and organisational measures. Without exposing sensitive operational details, the policy can explain implemented safeguards more meaningfully than 'we take reasonable security measures'.

It should also make rights usable: explain access to information, correction, erasure, grievance redressal and nomination, alongside request channels, privacy contacts and escalation routes. Retention deserves similar clarity: what is deleted when consent is withdrawn, what must remain, and why? Withdrawal requires processing to cease within a reasonable time, subject to lawful exceptions; erasure obligations also carry exceptions for legally necessary retention.

'Sharing with third parties' says little. Identifying relevant recipient categories like the cloud providers, payment processors or other vendors and explaining their roles is more useful. Although DPDP framework does not require a policy to list every destination country, explaining known overseas processing arrangements can improve transparency, while reflecting applicable transfer restrictions.

FOUNTAINHEAD LEGAL
C-2106, Oberoi Garden Estate, Chandivali Farm Road, Powai - 400072
T. +91 98338 62234 E. rashmi@fountainheadlegal.com
www.FountainheadLegal.com

Employees are another audience. A Data Fiduciary may choose an external policy and a separate internal policy, accessible through its intranet. The latter can explain employee-data practices and help staff understand the privacy standards expected in their work. Both should reflect consistent underlying practices.

There is also an evidentiary dimension. Given the Data Protection Board's document-production and inspection powers, a dated policy could help establish what the organisation represented at a particular time. This is a practical inference, not a statutory guarantee: the policy alone cannot prove compliance. Unsupported promises may instead expose gaps between stated and actual practices. Retaining previous versions therefore matters.

Policies should be reviewed periodically and whenever practices change. Borrowing a GDPR-regulated sister concern's policy requires particular care. A reference to age thirteen may reflect a national GDPR threshold for consent to certain online services; GDPR's default is sixteen, with permitted reductions to thirteen. India's DPDP framework covers children below eighteen.

The phased transition offers time to map processing, review processors, establish retention practices and organise rights handling. The resulting policy should give individuals useful answers and the organisation an accurate record of its commitments. Its value under DPDP framework will depend on how faithfully those commitments describe everyday practice.

FOUNTAINHEAD LEGAL
C-2106, Oberoi Garden Estate, Chandivali Farm Road, Powai - 400072
T. +91 98338 62234 E. rashmi@fountainheadlegal.com
www.FountainheadLegal.com