Is your website DPDA Compliant? A practice checklist for business

Introduction: The Growing Importance of Data Privacy in the Digital Economy

The digital economy has grown so fast that it has radically changed the way companies interact with consumers. Today most websites are not just ad-hoc sources of information. Every day people's data in the shape of contact details, cookies analytics, payment gateways, newsletters, customer registration, and so on is being constantly harvested, stored, and analyzed to optimize products and services and to boost advertising. Still, digital data is commercialised, it also brings about issues related to privacy, cyber-security, trespassing, and abuse of personal information. Customers are more and more aware of their rights and demand information about the collection of their personal data. That means, governments in many countries adopted tighter legislation on data protection, mostly in the digital media (Government of India, 2023).[1]

India sought to respond to these issues via passing the **Digital Personal Data Protection Act, 2023 (DPDPA)**, a legislation that defines the structure for the processing of digital personal data. It creates responsibilities for organizations to process such data and brings rights to individuals about its use. India's constitutional protection of privacy rights was greatly strengthened by the Supreme Court when it came to ***Justice K. S. Puttaswamy v. Union of India***[2]. In that pivotal case, the nine-judge bench unanimously held that the Constitutional right to privacy is implicit under Article 21 of the Constitution of India[2]. The court's judgment focused on informational privacy, dignity and autonomy, and set the precedent for the now-established Indian approach to data protection.

Evolution of India's Data Protection Framework and the Emergence of the DPDPA

Before the DPDPA came into operation, India never had a dedicated privacy legislation of its own. The data protection obligation was governed by provisions in the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These provisions, in turn, were often labeled as vagrants. Following the landmark judgment of the Supreme Court in Justice K. S. Puttaswamy v. Union of India, the question of a stronger privacy legislation came to the fore front the Government of India set up **Justice B. N. Srikrishna Committee** to look into questions of data protection and recommend a comprehensive legislation[3]. The Committee made its reportA Free and Fair Digital Economy: Protecting Privacy, Empowering Indians and the draft Personal Data Protection Bill in 2018. In the subsequent years, various draft data protection laws were introduced and discussed intensely. Parliament and the public debated on issues ranging from whether there should be a prior consent mechanism or an opt-in/ opt-out one, whether government exemptions should be permissible and restrictions on data transfers abroad to whether digital intermediaries should be held accountable and whether the digital economy should be subjected to specific requirements.
Finally, the Digital Personal Data Protection Bill, 2023 was enacted to provide a comprehensive law for the digital personal data of India[4].

The Act defines the category of 'Data Fiduciaries' as any organization or person who determines the purpose and means of processing of personal data. Data Principals are the individuals whose data is being processed by the Fiduciaries. Key user rights granted by the Bill include access correction erasure, grievance redressal, and right to withdraw the Consent.

---

[1] Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice. Government of India Gazette Notification.
[2] *Justice K. S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[3] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Government of India.
[4] Government of India. (2023). Digital Personal Data Protection Act, 2023. Ministry of Law and Justice.

Essential Requirements for Making a Website DPDPA Compliant

One of the most important factors that is significant in establishing that a breach has occurred under the DPDPA is the privacy policy that is in operation. A privacy policy that is explicit and accessible to the user will obviously satisfy the transparency requirement. Any privacy policy that is not clear or is hidden will probably breach the requirement that information be made available and could constitute contravention of the Act.

To ensure greater transparency, a compliant website should ideally provide users with the following information in a structured and accessible manner:

- What categories of personal data are being collected
- Why the information is being collected
- Whether the data will be shared with third parties
- How long the information will be retained
- The rights available to users regarding their personal data

Consent also forms a central aspect of lawful data processing under the DPDPA. Businesses must ensure that consent obtained from users is free, informed, specific, unconditional, and unambiguous[5]. Accordingly, websites should avoid deceptive mechanisms such as pre-ticked consent boxes, hidden clauses, or bundled authorizations that fail to properly inform users regarding the nature and purpose of data collection. Users must clearly understand what information is being collected and how it will be used before valid consent can be established.

Certain practices are increasingly viewed as inconsistent with valid consent standards, including:

- Pre-selected cookie acceptance boxes
- Automatically opting users into marketing communications
- Consent requests hidden within lengthy terms and conditions
- Vague authorizations permitting unrestricted data sharing.

A further fundamental requirement would be complying with the data minimization and purpose limitation principle. No superfluous or irrelevant data that does not serve a lawful business purpose should be gathered. For a plain newsletter subscription no more than an email address should suffice, and not detailed personal data such as demographics or justifications of one's identity.

Gathering superfluous data would be more liable and vulnerable to informatics system hacks. Many websites also use cookies, analytics tools and other tracking technologies to track user behavior online and make the user experience more targeted. Companies that without the user’s knowledge employ tracking technologies that could infringe on the privacy rights of the individual have serious privacy implications and these disclosures need to be made via cookie notifications and other appropriate notice requirements.
Common tracking technologies requiring disclosure include:

Browser cookies

[5] Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act, 2023: Overview and Key Provisions. Government of India.

- Website analytics tools
- Advertising trackers
- Location monitoring systems
- Behavioral profiling technologies

Cybersecurity protection measures are also a vital aspect of DPDPA compliance. The Act mandates that regulations be adopted by undertakings for protecting personal information through means of appropriate security measures to prevent access misuse breach or theft of data. While not an exhaustive list, these measures could comprise of encryption technologies, firewall protection, layered authentication techniques, multi-level authentication, penetration testing, and regular cyber-security monitoring. In today's day and age, the integration of cybersecurity into informational privacy protections in Justice K. S. Puttaswamy v. Union of India is well-established[6].

In practice, businesses are increasingly expected to adopt measures such as:

- Multi-factor authentication for user accounts
- Regular cybersecurity and vulnerability audits
- Encryption of sensitive financial and personal information
- Restricted employee access to confidential user data
- Timely reporting and management of data breaches

Businesses must additionally establish grievance redressal mechanisms enabling users to exercise their statutory rights effectively. Individuals should be able to access their personal information, seek corrections, request deletion or erasure, withdraw consent, and raise complaints regarding unlawful processing activities. Websites should therefore provide accessible grievance channels and clearly identify responsible officers or contact persons.

Legal Consequences of Non-Compliance and Business Liability Under the DPDPA

Adhering to the DPDPA is themselves becoming more than just good corporate practice but an expansion of the legal business requirement. Failure to approach privacy and data protection obligations will have legal, financial and reputation risks. A failure to institute reasonable security measures, processing personal data unlawfully, failure to comply with statutory obligations or failure to deal with rights of users and individuals satisfactorily could bring organizations incurring significant financial penalties under the DPDPA. Data Breach could also attract regulatory pursuits, loss of public confidence hacking adverse public opinion and a loss of confidence in the business.

The increased focus on digital accountability has also drawn the attention of courts and has led to jurisprudence on challenges to online governance and intermediary accountability. An example of this is the case of Shreya Singhal v. Union of India, in which the Court addressed issues on free speech and intermediary liability in the digital arena[7]. While the judgment was largely on a challenge to s. 66A of the Information Technology Act, it was significant to the larger debate on digital governance, platform accountability and constitutionality. Failure to comply could bring a loss of trust from consumers in a marketplace which is continuously becoming more competitive.

[6] *Justice K. S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[7] *Shreya Singhal v. Union of India,* (2015) 5 SCC 1.

Today’s consumers are more inclined to trust companies that are transparent, accountable and take responsibility for the data they have collected about them. As a result, privacy compliance is not just a legal duty but has become a vital issue for modern companies' management and good business[8].

Conclusion: Building Consumer Trust Through Responsible Data Governance

The Digital Personal Data Protection Act, 2023 is a significant step forward in an ever-growing digital legal environment in India. Given the proliferation of websites across businesses daily processing massive amounts of personal data, privacy compliance can no longer be an afterthought. A truly compliant website is not just a website with a privacy policy. To truly be compliant, it takes organizations to be committed to a broader organizational commitment to transparency, informed consent, information security, accountability, and responsible data management. Organizations need to actively look at their collection of data, enhance the security measures, implement grievance redressal systems, process data legally etc.

The designation of privacy as a fundamental right in Justice K. S. Puttaswamy v. Union of India shows that safeguarding personal data has become entangled with the very fabric of the Indian constitution, consumer confidence and corporate accountability. Over time, DPDPA-conscious enterprises not only decrease their legal liabilities, but also reinforce credibility, bolster their cybersecurity robustness and sustainably garner the confidence of Indian consumers in the liberalizing digital economy.

[8] Organisation for Economic Co-operation and Development. (2023). Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies.