INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 6 [2026] | Page 466 – 474

REGULATING THE DIGITAL BAZAAR: E-COMMERCE OBLIGATIONS UNDER INDIA'S DATA PROTECTION LAW

-Satviki Agnihotri[1]

Before we look at the provisions of the Digital Personal Data Protection Act ["DPDP Act"] we must begin by understanding what the term E – Commerce means. Section 2(16) of the Consumer Protection Act, 2019 defines "e-commerce" as buying or selling goods or services including digital products over digital or electronic networks. This definition is activity based rather than entity based, meaning that any entity engaging in the online sale of goods or services falls within the scope of e – commerce, irrespective of whether such sale is conducted exclusively online or alongside offline modes of business. Thus, firms that operate through both physical stores and digital platforms are not excluded from the regulatory framework governing e – commerce mainly due to their hybrid nature.

The Consumer Protection (E-Commerce) Rules, 2020 clarify the regulatory framework further by defining the term "e-commerce entity." According to Rule 3(b), an "e-commerce entity" means any person who owns, operates or manages digital or electronic facility or platform for electronic commerce, but does not include a seller offering his goods or services for sale on a marketplace e-commerce entity. Therefore, the rules broaden the scope of e-commerce entities beyond just Amazon and Flipkart to include all entities that operate independently of any other company using a digital interface for the purpose of conducting online commerce.

The Definition of Marketplace and Inventory Models under the Rules, for both Models, will be recognised as two major Models of E-commerce Businesses.

- A Marketplace E-commerce entity provides an information technology platform that facilitates transactions between Buyers and Third-party Sellers but does not own the inventory itself.
- An Inventory E-commerce entity will own the products and provide them directly to the Consumers through their own Digital Platforms.

[1] B.A. LL.B. (Hons.) | Semester V | National Law University, Jodhpur

As per the Rules of E-commerce, both Marketplace and Inventory Models are considered as E-commerce Entities, and both Models are subject to compliance obligations to ensure transparency, grievance redressal, consumer protection obligations, etc.

Based on this distinction, Lenskart and Croma, who sell products/goods directly via its website/application, are both classified as Inventory E-commerce Entities, as both are the Owners of the Digital Platforms that facilitate the sale of their Products via E-commerce. The presence of a brick-and-mortar retail operation does not change that categorisation. The ownership and operation of the Digital Interface that facilitates E-commerce transactions is the determining factor for categorising them as E-commerce Entities. However, when these same companies sell their products through third-party marketplaces like Amazon or Flipkart, their role in such transactions is limited to that of a "seller" on a marketplace, and not that of an e-commerce entity for those specific transactions.
Thus, Using the term "e-commerce entities" and not merely "Platforms" aligns with the language of the Consumer Protection (E-Commerce) Rules, 2020 and avoids the erroneous implication that only marketplace operators are capable of being regulated as digital commerce actors.
As far as the Significant Data Fiduciary ["SDFs"] status is concerned it does not depend on whether an entity is a marketplace like Amazon or a brand selling through its own website like Lenskart or Croma. What matters is the scale, sensitivity, and risk involved in the personal data being processed. If an e-commerce company whether a marketplace or an inventory-based seller processes large volumes of user data, handles sensitive personal data such as health, financial, or location data, or engages in profiling or large-scale tracking that could significantly impact individuals' privacy, the Central Government may notify it as an SDF. Therefore, companies selling both online and offline may also be classified as SDFs if their data practices meet the statutory risk thresholds, while merely selling goods online does not, by itself, make an entity an SDF.
Taking that as our premise we would analyse the same in light of the DPDP Framework.

LAWFUL BASIS AND CONSENT FOR PROCESSING PERSONAL DATA IN E-COMMERCE

(Section 6 read with Section 7 of the DPDP Act, 2023)

Under the DPDP framework, an e-commerce platform acts as a Significant Data Fiduciary (which according to section 10 is notified by the Central Government based on six *inter alia* relevant factors, which are - (a) the volume and sensitivity of personal data processed; (b) risk to the rights of Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order.) and can process personal data only when such processing is grounded in a lawful basis. Section 6 mandates that personal data must ordinarily be processed based on free, specific, informed, unconditional and unambiguous consent, expressed through a clear affirmative action. In the e-commerce ecosystem, this consent is typically obtained when a user creates an account, places an order, saves an address, or opts for digital payment. *For instance*, when a customer signs up on an online marketplace and consents to the processing of her name, phone number, email address and delivery location, the platform may lawfully process such data for account creation, order fulfilment and customer support.

However, consent in e-commerce is purpose specific. While a customer may consent to receive transactional updates relating to her order, such consent does not automatically extend to unrelated processing such as targeted advertising or sharing data with tIf an e-commerce platform uses a customer's delivery address to infer purchasing power or location-based profiling without explicit consent, such processing would violate Section 6.

Illustration – An e-commerce site may receive an order from a customer who has given consent to process their mobile number and email address only for the purpose of order confirmation, shipping notice, delivery updates, generating an invoice and support related to the customer's specific order, i.e. the consent would be applicable only in relation to that particular order. This consent will only allow transactional communications and will not allow a site to use those records for targeted behavioural or promotional advertising, as well as create profiles for marketing analytical purposes or share that information with third party advertisers, ad-tech platforms and data brokers, unless the customer has provided separate, explicit and specific written consent for each one of those activities. If an e-commerce platform uses a customer's delivery address for any other purpose than fulfilling that order and without the customer's explicit permission then the e-commerce platform has violated the DPDP Act, specifically sections 6 and 7, by processing data based on purposes that were not approved.

In addition to consent-based processing, Section 7(a) permits processing for "certain legitimate uses" where the Data Principal has voluntarily provided personal data for a specified purpose and has clearly

consented. In an e-commerce setting, this applies where a customer provides her mobile number to receive OTPs, delivery updates or digital invoices.

Illustration – When a user provides their phone number to receive real-time delivery tracking messages, the platform may process that data for logistics coordination. However, once the delivery is completed and the return window expires, continued processing of that data for unrelated purposes, such as unsolicited promotional calls, would be impermissible.

Section 7(b) becomes relevant where e-commerce entities act as digital intermediaries for State benefits or services. For example, during government welfare initiatives, certain entities may facilitate the delivery of subsidised goods or act as onboarding portals for beneficiaries. In such cases, the platform may process personal data where the user has previously consented or where the data is sourced from government-notified databases, provided such processing adheres to prescribed data governance standards.

Sections 7(c) to 7(e) allow processing for sovereign, statutory and judicial purposes. In the e-commerce context, this includes disclosure of transaction details to statutory authorities for tax compliance, sharing information with law enforcement agencies pursuant to lawful orders, or complying with court-directed disclosures and enforcements, in consumer disputes or contractual claims. Similarly, Sections 7(f) to 7(h) permit processing without consent in situations involving medical emergencies, public health crises or disasters. *For example,* during a pandemic or natural disaster, an e-commerce platform may process customer location and contact details to prioritise delivery of essential goods or to coordinate with emergency response agencies.

Section 7(i) permits processing of employee personal data by e-commerce companies for employment-related purposes, such as payroll processing, access control, prevention of data leaks, and protection of proprietary algorithms and customer databases.

NON-DELEGABLE RESPONSIBILITIES OF E-COMMERCE ENTITIES AS DATA FIDUCIARIES

(Section 8 of the DPDP Act, 2023)

Section 8(1) places a non-delegable obligation on e-commerce entities to comply with the DPDP Act in respect of all personal data processed by them or on their behalf. This is particularly significant in the e-commerce ecosystem, which relies heavily on third-party Data Processors such as delivery partners, payment gateways, cloud service providers, analytics vendors and outsourced customer

support teams. Even where a data breach or misuse occurs at the level of a logistics partner or payment processor, the primary responsibility remains with the e-commerce platform as the Data Fiduciary.

Illustration – Pursuant to section 8(1), an e – commerce platform ["Entity A"], acting as the data fiduciary, collects a customer's name, delivery address and mobile number for order fulfilment. For the specific purpose of execution of the transaction, Entity A engages an independent logistics provider ["Entity B"] to whom delivery details are disclosed, and a third party payment gateway ["Entity C"] to whom payment related personal data is transmitted, each functioning as Data Processors. In the event of unauthorised access, misuse, or a personal data breach occurring at the level of Entity B and Entity C, the processing remains governed by the DPDP act and the obligation to ensure compliance continues to rest with Entity A under Section 8(1), notwithstanding the delegation of processing activities.

Section 8(2) further mandates that Data Processors may be engaged only under valid contracts which are referred to as the Data Processing Agreements ["DPAs"]. In practice, this means that contracts with delivery companies as well as vendors must clearly restrict access to only necessary data, such as delivery addresses and contact numbers, and prohibit access to payment details or browsing history. Similarly, contracts with cloud service providers must mandate compliance with DPDP level security standards and impose obligations relating to breach reporting and audit cooperation.

Under Section 8(3), e-commerce entities must ensure the accuracy, completeness and consistency of personal data where such data is used to make decisions affecting customers or is shared with other Data Fiduciaries. For instance, if incorrect address data leads to wrongful order cancellation or denial of a refund, the platform may be held accountable. Likewise, where customer data is shared with banks or Buy-Now-Pay-Later ["BNPL"] providers for credit assessment, inaccurate data could materially prejudice the customer and violate statutory obligations.

Under Section 10(2), an SDF has additional compliance obligations due to the large volume of sensitive data being processed, and this becomes pertinent for E – Commerce entities as they have a large share of Data Principals to cater to. An SDF must appoint a data protection officer ["DPO"], The DPO needs to be hired/designated and is an individual based in India and accountable to the board of directors, or the equivalent governing body, and represents the SDF under the DPDP Act. The DPO, who is required to be based in India, functions as the primary grievance redressal contact for data principals, oversees compliance with the DPDP Act and internal data protection policies, and reports directly to the board or governing body of the SDF. Further, the DPO facilitates and advises on Data Protection Impact Assessments ["DPIAs"], supports the exercise of data principal rights such

as access, correction, and erasure, conducts privacy training and awareness programs for employees, and acts as the key interface between the organisation and the Data Protection Board of India, thereby ensuring effective regulatory engagement and accountability. The DPO serves as the primary point of contact for grievance redressal and acts as an effective bridge for communication between data principals and SDFs. Also, the SDF must appoint an independent data auditor to conduct regular audits of data and evaluate compliance with statutory obligations. Additionally, the SDF must perform periodic DPIAs once in every period of twelve months (12 months) from the date on which it is notified as such or is included in the class of Data Fiduciaries notified as such, as is provided under rule 13 of the DPDP Rules, to identify, evaluate and reduce risks, related to the rights of data principals that may arise from the SDF's processing of their personal data, in order to comply with the Digital Personal Data Protection Act and any other applicable regulations. In addition to performing DPIAs, the SDF must also conduct periodic audits, and implement any other measures prescribed under the Act.

SECURITY SAFEGUARDS AND PROTECTION OF CUSTOMER DATA

(Section 8(4) and 8(5) read with Rule 7 of the DPDP Rules, 2025)

Sections 8(4) and 8(5) impose a duty on e-commerce entities to implement appropriate technical and organisational measures and to take reasonable security safeguards to prevent personal data breaches. Rule 7 of the DPDP Rules, 2025 operationalises this obligation by prescribing minimum security standards.

In the e-commerce context, this requires entities to secure sensitive data such as payment credentials, saved addresses and identity details through encryption, masking or tokenisation. *For example*, an e-commerce platform must ensure that customer card details are tokenised and never stored in raw form, even when processed by payment gateways. Access to backend databases must be strictly role-based, ensuring that delivery partners can view only delivery addresses and customer support agents can access only limited order-related information.

Rule 7 also requires maintaining visibility over data access through logging and monitoring. For instance, if an employee accesses an unusually high number of customer profiles, system logs must enable detection and investigation of potential misuse. E-commerce entities must further ensure business continuity through regular backups and disaster recovery mechanisms so that essential

services such as order tracking, refunds and customer support remain functional even in the event of cyber-attacks or system failures.

Rule 8(3) provides that access logs and relevant personal data must be retained for a minimum period of one year (1 year) from the date of processing, for the purposes listed in the Seventh Schedule, before erasure (unless a longer period is required by law), enabling post-incident investigation and regulatory scrutiny. Contracts with Data Processors must include explicit security obligations, and organisational measures such as employee training, internal audits and compliance reviews must be undertaken. The definition of "computer resource" under Rule 7(2), borrowed from the IT Act, 2000, ensures that the entire digital infrastructure of the e-commerce platform servers, cloud systems, databases and networks falls within the security framework.

INTIMATION OF PERSONAL DATA BREACHES IN E-COMMERCE

(Section 8(6) read with Rule 6 of the DPDP Rules, 2025)

Section 8(6) mandates that e-commerce entities must notify personal data breaches, and Rule 6 of the DPDP Rules, 2025 prescribes the manner of such intimation. Upon becoming aware of a breach such as leakage of customer addresses or phone numbers the platform must inform affected customers (Data Principals) without delay, in clear and plain language, through their user accounts or registered communication channels. The intimation must explain the nature and timing of the breach, the likely consequences such as phishing or fraud, the mitigation measures taken, and the safety steps customers may adopt, such as changing passwords or monitoring bank statements. There is no clear time limit prescribed to do so, unlike in the case of the Data Protection Board. For E- commerce entities informing the Data Principals becomes very important and hence the requirement of the breach notices.[2]*

Simultaneously, the platform must notify the Data Protection Board ["DPB"] without delay and submit a detailed report within seventy – two hours (72 Hours). In the e-commerce context, this report would typically include details of whether the breach occurred due to a compromised seller account, a third-party logistics partner, or an internal system vulnerability, as well as measures adopted to prevent recurrence.

While the period for intimation to the Data Principals has not been specified, since the data is being made available to the DPB within 72 hours, which means it is in the public domain, it is advisable that the platform informs the Data Principals also within that time as that would be both reasonable and prudent.

DATA RETENTION, ERASURE AND DEEMED EXPIRY OF PURPOSE

(Section 8(7), 8(8) and 8(11))

Section 8(7) requires e-commerce entities to erase personal data upon withdrawal of consent or once the specified purpose is no longer served, unless retention is required by law. For example, while order and payment records may need to be retained for tax or consumer protection compliance, storing customer browsing history indefinitely without justification would violate the Act. The obligation to erase data also extends to ensuring that Data Processors delete data shared with them.

Section 8(8) introduces the concept of deemed expiry of purpose, under which personal data must be erased if a customer does not place orders or exercise data rights for a prescribed period. Section 8(11) clarifies that a customer is considered inactive where she has not logged in, placed orders or contacted customer support. This prevents indefinite hoarding of dormant customer data by e-commerce entities.

The Ministry of Electronics and Information Technology has mandated that e – commerce companies and social media intermediaries with more than 20 million registered users in India, must delete a user's personal data if the individual has not accessed the service, placed an order, or contacted support for three consecutive years (3 years). Prior to deletion, intermediaries are required to provide the individual with a 48-hour notice, allowing them to log in and retain their data. In Addition, SDF platforms with more than 5 million registered users must conduct an annual audit and a DPIA to ensure ongoing compliance with the Act. These platforms are also required to verify annually that the technical measures, including algorithms

TRANSPARENCY AND GRIEVANCE REDRESSAL IN E-COMMERCE ENTITES

(Section 8(9) and 8(10) read with Rule 8 of the DPDP Rules, 2025)

Section 8(9), read with Rule 8, requires e-commerce entities to publish clear contact details of the Data Protection Officer or an authorised grievance officer. This enables customers to seek clarification or raise concerns regarding the processing of their personal data. Section 8(10) further mandates the establishment of an effective grievance redressal mechanism, allowing customers to raise complaints relating to consent withdrawal, data misuse, excessive retention or breaches before approaching the Data Protection Board.

CONCLUDING ANALYSIS

Read together, Sections 6, 7 and 8 of the DPDP Act, 2023 and Rules 6, 7 and 8 of the DPDP Rules, 2025 create a comprehensive regulatory framework governing e-commerce platform. The framework recognises the commercial realities of digital marketplaces while imposing strict obligations relating to lawful processing, security, accountability, breach transparency and data minimisation. In doing so, it seeks to balance innovation in e-commerce with the fundamental right of individuals to informational privacy.