LEGAL LOCK JOURNAL

2583-0384

VOLUME 3 || ISSUE 3

2024

IMPACT OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023 ON INDIAN E-COMMERCE

Pavan Krishna Chimmili[1]

ABSTRACT

The right to privacy is a fundamental right that includes the data of a person. There are many e-commerce intermediaries in India that provide different types of services to the data principles by processing their data. The regulation of data processing by e-commerce intermediaries is always a major concern in India, as they are the data fiduciaries who process the data according to the principles of marketing and analytics, but not after the enactment of the Digital Personal Data Protection Act, 2023.

There is a huge impact on these e-commerce intermediaries as the newly enacted law addresses several data protection principles. Before the enactment of this act, most e-commerce intermediaries did not consider consent while processing the data. Now, there should be specific consent from the data principles, and a mandatory notice of why the e-commerce intermediaries are processing the data should be given to the data principles.

The purpose of this paper is to determine the impact of the Digital Personal Data Protection Act, 2023, on e-commerce intermediaries in processing the data under the data principles. Different types of procedures and innovative techniques have to be followed by e-commerce intermediaries to comply with the provisions of the newly enacted data protection law of India. To observe the impact of this newly enacted law on e-commerce intermediaries, the researcher follows the analytical method of research in this paper.

Keywords: Data principle, Data fiduciary, Privacy, Intermediary, E-commerce.

INTRODUCTION

The objective of the Digital Personal Data Protection Act, 2023 is that the personal data should be processed fairly and lawfully. The legislations of different countries does not provided express protection for data on e-commerce intermediaries. Data protection laws are important because people should have trust in order to buy products and services from

[1]The author is a student of Damodaram Sanjivayya National Law University.

companies and this trust plays a crucial role in business.[2] The Digital Personal Data Protection Act, 2023, has been enacted mainly for two reasons. The first reason is the inability of the existing laws to address data protection issues, and the second reason is to tackle the problems related to data protection and privacy.

The purpose of the data protection law is to protect the interests of both data principals and data processors by upholding the legitimate processing of both. Before 1979, people used to buy products and services directly from the company itself. The total business was between the customers and the companies that were offering those products and services.

During the course of time, companies have discovered that they cannot do everything alone. For instance, in the 1970s, Intel released the world's first dynamic RAM chip, which has a capacity of 1024 bits. If they want to sell these products to all the needy people, they need a number of middlemen for the smooth functioning of their business. In 1979, Michael Adrich invented electronic shopping, and he is considered the founder of e-commerce.[3] From 1979 to 2024, there has been tremendous growth in the e-commerce industry, where people are buying the products and services of different companies through e-commerce intermediaries.

Section 2(1)(w) of the Information Technology Act, 2000, defines the term "intermediary." The definition includes 'online-market places', by which we can understand that e-commerce giants like Amazon, Flipkart, Zomato, etc. fall under the definition of intermediary. At present, e-commerce intermediaries in India collect so much information about the data principals (consumers) of companies to offer many products and services from different companies. These companies process a lot of data from these sources, like personally identifiable information, sensitive information for the smooth functioning of their businesses, and consumer needs. There are chances that these companies can sell the data they have collected to others.

GROWTH OF E-COMMERCE IN INDIA

The growth trajectory of e-commerce in India is upward. There are more than 80 million Internet users in India, and the number of online shoppers may increase to 4.27 million.[4]

[2] LA Bygrave, Data Protection Law: Approching its Rationale, Logic and Limits (Kluver Law International 2022) chs 3 and 8.
[3] M. Aldrich, Online Shopping in the 1980s, (IEEE 'Annals of the History of Computing) 33 at pp57.
[4] E-commerce surge: India to add 80 million online shoppers by 2025, (LIVE MINT) (April 21, 2023) https://www.livemint.com/industry/energy/igx-acme-tie-up-to-develop-green-hydrogen-and-ammonia-market-in-india-11707485691651.html (last accessed on January 20, 2024).

At present, online shopping is becoming a common mode of shopping among most Indians. E-commerce adoption is close to 100% of pin codes in India. With so much of growth rate, the e-commerce market in India is expected to reach more when compard to the present market.[5]

By 2026, it is expected that Indian e-commerce will have grown to US$ 163 billion at a compound annual growth rate (CAGR) of 27%. The gross merchandise value (GMV) of online sales increased by 22% to US$ 60 billion in the financial year 2022–2023 from the previous financial year. The gross margin on e-commerce was US$49 billion in FY22. By 2030, the business-to-business (B2B) internet marketplace in India is expected to generate US$200 billion in opportunities. India had more than 800 million users and 125.94 lakh crore UPI transactions in 2022, making it the world's second-largest internet market.

According to Deloitte India Report[6], Indian sub-continent is expected to become the one of the biggest consumer market in the world, and the country's online retail market is expected to grow, primarily because of the country's tier-2 and tier-3 cities seeing rapid e-commerce expansion. Tier-3 cities' proportion in the e-commerce market increased from 34.2% in 2021 to 41.5% in 2022.

By 2025, Grant Thornton projects that India's e-commerce industry will have a valuation of US$188 billion.[7] Simultaneously, the reason for the growth of e-commerce intermediaries is the data they are relying on and processing. They cannot do business without collecting data from the data principals.

PERSONAL DATA

Personal Data is a valuable asset but if one wants to protect it, one needs to know what it is.[8] Whenever a data principal is searching for any product or service in the marketplace of an e-commerce intermediary, he or she has to login and provide personal details. This personal data includes identifiable information, which can be classified into four types of data[9].

[5] E-Commerce Industry Report, (IBEF), (August, 2023), https://www.ibef.org/industry/ecommerce-presentation (last accessed on Janaury 20, 2024).
[6] Anand Ramanathan, Future of Retail: Emerging Landscape of Omni-Channel Commerce in India, (DELOITTE), (June 27, 2023), https://www2.deloitte.com/in/en/pages/about-deloitte/articles/future-of-retail-emerging-landscape-of-omni-channel-commerce-in-India.html (last accessed on 20 January, 2024).
[7] Sarala M Mary, Growth of e-commerce in India, 4 (IRJETS).
[8] Jeroen Van Den Hoven, Technology, "Privacy and of Personal Data" in Technology and Moral Philosophy, Jeroen van den Hoven and John Weckert (eds)301-321, Cambridge University Press (2008).
[9] Classification of four types of Personal Data is based on the examination of privacy policies of Amazon, Flipkart and Zomato.

Basic Data

Basic data is the name, address, phone number, age, location (to provide better service on the basis of location), IP address of the mobile or computer used by the data principal, E-mail address (through which the entire communication happens if the data principal has opted for it); Phone number (through which one-time passwords for bank transactions and identification links to the account will be communicated); Officially valid documents like the Aadhar Card, Pan Card, and bank account details of the data principal.

Interaction Data

Interaction data are the contacts of the data principal (through which there will be easy transfer of money to other accounts or giving access to the contacts the data principal can invite others to use the e-commerce platform); Names of the people, addresses of friends, and other people.

Behavioural Data

Behavioural data is the content review of the products and services; Photograph of the data principal; Voice recordings (if the data principal has used the voice search option); Wi-Fi credentials; description, which has been mentioned in the profile; Images and videos were collected and stored with the e-commerce intermediary.

Attitudinal Data

Attitudinal data is the opinion of the data principal about the respective products and services. This type of data is collected through ratings and surveys.

OBLIGATIONS OF E-COMMERCE INTERMEDIARY

The relationship between the data principal and the data fiduciary is a fiduciary relationship, where the data principal places trust, reliance, and confidence in providing the products and services.[10] The Digital Personal Data Protection Act, 2023, provides

Amazon.com Privacy Notice, (AMAZON), (August 11, 2023), https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (last accessed on January 16, 2024).
Privacy Policy, (FLIPKART), https://www.flipkart.com/pages/corona-privacy-policy#:~:text=We%20may%20disclose%20personal%20information,violates%20the%20rights%20of%20a (last accessed on January 16, 2024).
Privacy Policy, (ZOMATO), (April 22, 2020), https://www.zomato.com/policies/privacy/ (last accessed on January 16, 2024).

[10] Tamar Frankel, Fiduciary Law, California Law Review, Vol. 71, No. 3, p. 795, (1983) https://www.jstor.org/stable/3480303 (accessed on January 31, 2024).

some basic principles of data protection, which are about the general obligations of the data fiduciary.

Fair and reasonable processing

The existence of the fiduciary relationship between the data principal and the data fiduciary is premised on the relationship between them, and in order to fulfil the objectives of the data fiduciary, it may lead to abuse of power.[11] In a contract, there will be unequal bargaining power, but in this fiduciary relationship, there is the dependence of one party on the other. In order to curb this abuse of power, Section 8(1) of the Act[12] says that the data fiduciary shall be responsible for any data processing by complying with the provisions of the DPDP Act, 2023. Duty of care, irrespective of the exact nature of the relationship, should be followed in order to fulfil the objectives of the Act.

Data Minimization and Purpose Limitation

E-commerce intermediaries collect data for different purposes. In order to fulfil those purposes, they may seek the assistance of third-party intermediaries. The collection of data by the data fiduciary from the data principal occurs on a large scale; in 2016, over 16.1 zettabytes of data were generated.[13] The purpose may be for financial transactions or communication of acceptance by email. Section 7(a) of the Act[14] says that the data fiduciary has to process the data that has been voluntarily provided by the data principal, but they should not process any other data that has not been consented to by the data principal.

Transparency

Most of the data principals who are getting products and services from e-commerce intermediaries lack information on how the data is being processed by these companies, and they lack awareness on how to file a complaint with the Data Protection Board. In order to ensure transparency, Section 5 of the DPDP Act, 2023 says something about the notice. As stated above, to process the data, there will be a purpose. Whenever a data principal has consented to give data, a notice should be given for the purpose for which

[11] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, (2018), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed on Febuary 10, 2024).
[12] Digital Personal Data Protection Act, 2023, No. 22, § 8(1).
[13] Committee of Experts, White Paper of the Committee of Experts on a data protection framework for India, (2018), https://www.meity.gov.in/writereaddata/files/meity_om_constitution_of_expert_committee_31072017.pdf, (last accessed on February 2, 2024).
[14] Digital Personal Data Protection Act, 2023, No. 22, § 7(a).

the data is being processed. According to sub-section (4) of sections 6 and 13 of the DPDP Act, 2023, so many rights can be exercised by the data principal. It is the obligation of the data fiduciary to give notice about these rights. There can be a dispute, or a data principal may file a complaint with the data fiduciary. It is the obligation of the data fiduciary to give notice of the manner in which the data principal files a complaint with the Data Protection Board.

E-COMMERCE INTERMEDIARIES ARE GETTING READY FOR PERSONAL DATA PROTECTION IN INDIA.

The Digital Personal Data Protection Act was notified in the official gazette on August 11, 2023. The formation of the Data Protection Authority of India and the rules of the same are still in the process. The main important question is whether the e-commerce intermediaries are getting ready for the personal data protection of their data principals or not. When the General Data Protection Regulation came into existence in 2018, companies were given about 2 years of buffer time to comply with the provisions of the GDPR. In India, e-commerce intermediaries should also be ready for the effect of the Act on them.

The International Association of Privacy Professionals (IAPP) and Ernst & Young (EY) conducted surveys in the European Union to know the privacy budgets and operations to ensure that they comply with GDPR. The survey of about 600 privacy professionals in 2016 who are working in industries with business-to-consumers (B2C) and business-to-business (B2B) models.[15] The results of the survey show that 35% of the companies are increasing their privacy budgets to comply with the privacy law. 50% of the companies have an intention to invest in privacy because of the privacy law. In 2017, IAPP and EY again conducted a similar survey after a year. The results of the survey show that spending on privacy in their budget has increased from $1.7 million to $2.1 million.[16] There has been an increase in the investment made in the privacy budget by the companies. Companies are investing in privacy staff.

[15] IAPP-EY Privacy Governance Report 2016, (International Association of privacy Professionals), (2016), https://iapp.org/resources/article/privacy-governance-report/ (last accessed on February 3, 2024).
[16] IAPP-EY Privacy Governance Report 2017, (International Association of privacy Professionals), (2017), https://iapp.org/news/a/2017-iapp-ey-privacy-governance-report-released/ (last accessed on February 3, 2024).

E-commerce intermediaries in India also have to start increasing their privacy budget in order to comply with the DPDP Act, 2023, because the right to privacy is a fundamental right in India[17]. Therefore, a paradigm shift is required in the functionality of e-commerce intermediaries in relation to personal data protection.

POWERS OF THE DATA PROTECTION BOARD OF INDIA

According to Section 27 of the DPDP Act, 2023, the Data Protection Board of India can exercise powers and functions in the proceedings of a data protection case. The Board can inquire into a personal data breach and impose penalties after the intimation of a personal data breach by a data principal under sub-section (6) of Section 8 of the DPDP Act, 2023. The Central Government or a State Government can refer to enquire into any data breach by a fiduciary, and the Board can impose penalties. The Board can inquire into a complaint filed by the data principal in respect of the registration of the consent manager and a breach by the consent manager and can impose a penalty. The major power of the board is that they can impose a huge amount of penalty on data fiduciaries, which may extend to two hundred and fifty crore rupees.

PENALTY IMPOSED ON BREACH OF PROVISIONS OF THE DPDP ACT

According to the Schedule of the DPDP Act, 2023, the board may impose a penalty of two hundred fifty crore rupees when a data fiduciary doesn't take reasonable safeguards to prevent personal data breaches, as mentioned under sub-section (5) of Section 8 of the DPDP Act, 2023. If the data fiduciary failed to give notice to the data principal as mentioned under sub-section (6) of Section 8 of the DPDP Act, then the Board may impose a penalty of two hundred crore rupees.

Section 9 of the DPDP Act, 2023 provides obligations of the data fiduciary in relation to the personal data of the children. If there is any breach, and upon intimation by complaint by any data principal, the Board may impose a penalty of two hundred crore rupees. The Act recognises both the rights of the data principal and the data fiduciary. If the data principal fails to comply with the duties mentioned under Section 15 of the Act[18], then the Board may impose a penalty of about ten thousand rupees.

[17] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1.
[18] Digital Personal Data Protection Act, 2023, No. 22, § 15.

In India, we cannot find proceedings for any personal data protection case because the Government of India is still in the process of forming a Data Protection Board of India.[19] The General Data Protection Regulation (GDPR), which came into existence in 2018, is a stringent law in the field of personal data protection. There are so many cases filed before the data protection authorities of the European Union (EU), where they are imposing a huge amount of penalties on the data fiduciaries.

Different Data Protection Boards of the European Union have imposed huge amounts of penalties on e-commerce intermediaries like Uber and Amazon. On the basis of these cases, which will be discussed below, we can understand the impact of the new legislation on personal data protection in India.

CASE STUDY ON UBER B.V. AND UBER TECHNOLOGIES INC.

Uber is a global business that runs a ride-sharing service network that links drivers and passengers in their personal cars. Users can track the whereabouts of their designated driver and request rides via the smartphone app that connects them to the platform. The association "La Ligue des droits de l'Homme,[20]" which represents more than 170 French drivers on the Uber platform, has filed a collective complaint with the CNIL (Commission Nationale de l'Informatique et des Libertés), which is the Data Protection Authority of France, alleging difficulties they have in exercising their legal rights.[21]

Analysis

Given that Uber's principal place of business is in the Netherlands, the Dutch Data Protection Authority assumed responsibility for the investigations in accordance with the General Data Protection Regulation (GDPR), cooperating closely with the CNIL throughout the process. The evidence was examined and verified, in large part, by the CNIL. This cooperative effort persisted throughout the one-stop-shop procedure's assessment of the draft order.

[19] Ashutosh Mishra, DPDP rules to be out by January-end, says MoS IT Rajeev Chandrasekhar, Business Standard, (January 16, 2024), https://www.business-standard.com/india-news/dpdp-rules-expected-to-be-released-by-end-of-the-month-mos-chandrasekhar-124011600679_1.html (last accessed on February 6, 2024).

[20] William D. Irvine, Between Justice and Politics: The Ligue des Droits de l'Homme, 1898-1945, Stanford University Press, 288 (2017), https://www.jstor.org/stable/j.ctvr33cn9?turn_away=true (accessed on February 6, 2024).
June 1898 marked the founding of the 'Ligue des droits de l'homme' (League of the Rights of Man) in Paris.

[21] BDK Advokati, Uber judgment: On human involvement in automated decision-making, Lexology, (July 20, 2023), https://www.lexology.com/library/detail.aspx?g=5a54b39c-1225-493d-a125-1c85918b05ed (accessed on February 6, 2024).

Uber made it needlessly difficult for drivers to get copies of or access to their personal data, the DPA found. Even though the app had a form, it was buried deep inside and dispersed over multiple menus; it should have been in a more accessible spot.[22] Additionally, Uber neglected to mention in its privacy terms and conditions the precise security measures used when transferring drivers' personal data to organisations outside the European Economic Area (EEA) as well as the data retention duration. The DPA discovered that Uber had prevented its drivers from using their right to privacy. Among the found infractions are the following:

1) Providing information about processing activities solely in English and failing to give requested data in a form that is accessible under the right of access.
2) The online form that drivers use to exercise their rights is not sufficiently accessible.
3) Their privacy statement gives too generic information about data retention periods and provides insufficient information about data transfers beyond the EEA.

Penalty

Uber B.V. and Uber Technologies Inc. were fined ten million euros (89,41,80,000 Indian rupees) by the Dutch Data Protection Authority for many infractions involving driver information.[23]

CASE STUDY ON AMAZON

The e-commerce giant's warehouses in France are overseen by Amazon France Logistique, which receives, stores, and gets ready to deliver packages to consumers. Every warehouse worker receives a scanner as part of their work so that they can record, in real time, the completion of certain duties allocated to them (removing or storing an item from the shelves, packaging or putting away, etc.).[24] Every scan an employee performs generates data that is recorded, kept, and utilised to compute indicators that reveal details about each employee's productivity, quality, and inactive times. In response

[22] UBER: Dutch data protection authority imposes €10 million fine, (CNIL), https://www.cnil.fr/en/uber-dutch-data-protection-authority-imposes-eu10-million-fine (accessed on February 6, 2024).
[23] Piotr Lipinski, Dutch watchdog fines Uber 10 mln euros over privacy regulations infringement, (REUTERS), (february 1, 2024), https://www.reuters.com/technology/dutch-watchdog-fines-uber-10-mln-euros-over-privacy-regulations-infringement-2024-01-31/ (accessed on 6 february, 2024).
[24] Employee monitoring: French SA fined Amazon France Logistique €32 million, (European Data Protection Board), (January 23, 2024), https://edpb.europa.eu/news/national-news/2024/employee-monitoring-french-sa-fined-amazon-france-logistique-eu32-million_en (accessed February 6, 2024).

to news reports regarding the company's warehousing procedures, the CNIL conducted multiple investigations. Additionally, there were other grievances from the staff.

Analysis

The CNIL believed that the mechanism in place to keep an eye on worker performance and activity was overly onerous, namely for the reasons listed below. According to the CNIL, it was unlawful to set up a system that measured work disruptions with such precision, possibly necessitating that workers provide an explanation for each break or interruption. The CNIL has discovered multiple GDPR violations by Amazon France Logistique.

1) Not adhering to the GDPR's Article 5.1.C[25], which addresses data minimization.
2) Not ensuring that processing is permitted as per GDPR Article 6.[26]

Penalty

Amazon France Logistics has been fined €32 million (2,86,58,56,000 Indian rupees) by the CNIL's restricted committee, which is in charge of imposing penalties.[27]

There is a huge impact of GDPR on these intermediaries. Uber and Amazon are also doing their business in India as e-commerce intermediaries. Not only Uber and Amazon, but every e-commerce intermediary that is doing business in India has to comply with the DPDP Act, 2023.

DATA BROKERS

Personal data protection in India is at an alarming stage. The companies that collect personal information about people, do business by selling, licencing, and allowing another company to use that data are called data brokers.[28] The report of the data removal service ‘Incogni’ states that more than 1.8 million personal information records were breached through 10 data breaches, making India the second most affected data broker

[25] Article 5.1.C of the General Data Protection Regulation, 2018.
[26] Article 6 of the General Data Protection Regulation, 2018.
[27] CNIL Imposes €32 Million Fine on Amazon France Logistique for GDPR Violations, (GRC REPORT), (January 24, 2024), https://www.grcreport.com/post/cnil-imposes-eu32-million-fine-on-amazon-france-logistique-for-gdpr-violations (accessed on February 6, 2024).
[28] Jennifer Barrett Glasgow, Data Brokers: Should They Be Reviled or Revered?, Cambridge Handbook of Consumer Privacy, 2 (2018).

breaching country in the world.[29] The data broker companies in India are selling the personal information of people living in metropolitan cities for 10,000 to 15,000 Indian rupees.[30] If an e-commerce intermediary acts as a data broker for any other company, then they shall specifically mention the selling of data principals personal information to others and also should provide an option to withdraw from selling their personal information to other companies at any time.

TECHNOLOGICAL AND INSTITUTIONAL MEASURES

After the enactment of the DPDP Act, 2023, many changes came in the field of personal data protection in India. In order to comply with the provisions of the Act, e-commerce intermediaries should take some measures to avoid complaints. Those measures include:

Privacy Policy

The DPDP Act did not use the privacy policy, but it can be interpreted by reading Section 5 (Notice) and Section 6 (Consent) of the DPDP Act, 2023. A privacy policy of an e-commerce intermediary explains the data principal about the personal information collected by them through a mobile app or website.[31] If an e-commerce intermediary collects personal information about any data principal to process that data, then a privacy policy is important. The language used in the privacy policy should be clear and readable by the data principle. The purpose of a privacy policy is to protect the data principals from unfair means of data collection, and a good privacy policy helps an e-commerce intermediary by explaining how they may collect the data, the purpose of data collection, and how they will process that information. Cookies also fall under the ambit of personal data protection. They are small files that are stored in the hardware of a data centre so that they will track the website or app usage behavior. The use of cookies by data fiduciaries should also comply with the provisions of the Act.

The Claudette Project[32], which is a study conducted by the European Consumer Organisation, outlines the requirements of the privacy policies of companies to comply with GDPR. The study analysed about fourteen privacy policies of different companies

[29] Federico Morelli, brokers ramp up lobbying efforts, spending $143 million over three years, (INCOGNI), (2023), https://blog.incogni.com/data-brokers-lobbying/ (accessed on February 7, 2024).
[30] Soham Shetty, India among top 5 countries most affected by data broker breaches, report reveals, (CNBC TV), (March 10, 2023), https://www.cnbctv18.com/news/india-among-top-5-countries-most-affected-by-data-broker-breaches-report-reveals-incogni-16139021.htm (accessed on February 7, 2024).
[31] Korunovska Jana, Kamleitner Bernadette, The Challenges and Impact of privacy policy comprehension, Twenty-Eigth European Conference on Information Systems (ECIS2020), Marrakesh, Morocco, (CORNEL UNIVERSITY), (2020).
[32] Francesca Lagioia, Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence, (SSRN Electronic Journal), (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3208596 (accessed on February 7, 2024).

that have huge markets around the world. They are Amazon, Apple, Google, Facebook, Microsoft, Twitter, WhatsApp, Uber, Booking.com, Airbnb, Epic Games, Netflix, Skyscanner, and Stream. The Claudette Project revealed that, out of these fourteen companies, none of their privacy policies are in compliance with GDPR. They have problematic processing clauses, unlawful clauses, and unclear language.

Data Protection by Design and Default

Every e-commerce app or website should have some privacy tools in order to protect against privacy risks. This methodology aims to protect against privacy attacks.[33] When any data principal wants to buy products and services from them, then the activities involved in the processing of that data should have appropriate security levels. If they want to build trust in data principals, then they have to show transparency in the collection of personal data, which should be understandable to the data principals.

Third-party services

An e-commerce intermediary can hire a third party for reasons like sending emails to the data principals and for financial transactions. Third-party service companies may save data or depend on that data to develop their businesses, thereby abusing their power.[34] Data fiduciaries have to ensure that every third party, whether directly or indirectly involved in the process of personal data collection, has to comply with the provisions of the Act.

Consent Manager

Every e-commerce intermediary shall have a consent manager. They should be registered with the Data Protection Board of India. According to sub-section 8 of Section 6 of the DPDP Act, the consent manager should have accountability and act according to the grievances of the data principals. Under sub-section 4 of Section 6 of the DPDP Act, 2023, a data principal has the right to withdraw consent at any time, which can be communicated to the concerned consent manager of that intermediary.

[33] Ann Cavoukian, Ph.D, Information & Privacy Commissioner, Privacy by Design The 7 Foundational Principles, (Internet Architechture Board), https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf (accessed on February 8, 2024).
[34] Piotr Foitzik, What you must know about 'third parties' under GDPR and CCPA, (IAPP), (November 29, 2019), https://iapp.org/news/a/what-you-must-know-about-third-parties-under-the-gdpr-ccpa/ (accessed on February 8, 2024).

Awareness for the Employees

Personal data protection is very crucial in the e-commerce industry. There may be chances of illegal methods of data processing by any employee. E-Commerce intermediaries, when they are recruiting employees, should have a strict non-discourse agreement by providing clauses that they will be liable for any infringement of the provisions of the DPDP Act, 2023.

CONCLUSION

There is a huge impact of the Digital Personal Data Protection Act, 2023, on e-commerce intermediaries. When we observe the privacy policies of e-commerce intermediaries, the language used is plain, unclear, and ambiguous. Every data fiduciary has to increase their budget for digital data protection because every data fiduciary should have a consent manager and fair and reasonable data processing techniques should be adopted. When any data principal opens the mobile application or website of any data fiduciary, they should get notice for data collection, and consent should be obtained from them. The intermediaries should follow technological and institutional measures in order to achieve the objectives of the DPDP Act. Indian personal data protection law is not as stringent as GPDR, but the penalty is so high if there is any infringement of the provisions of the DPDP Act, 2023.