NAVIGATING DATA PROTECTION LAWS: A COMPARATIVE STUDY OF THE GDPR AND INDIA'S DPDP ACT

BY VIDUSHI ANAND[1]

ABSTRACT:

Few years ago, privacy was not recognized as an essential element of human life. However, with the growth of technology and the rising cases of infringement of data, it was realized that every individual is entitled to privacy. In the famous case of Justice K.S. Puttaswamy vs Union of India (2018), 'Right to Privacy' was recognized as a fundamental right protected under Article 21 of the Constitution of India. By recognizing the right to privacy as a fundamental right, the Supreme Court took a significant step toward safeguarding an essential aspect of human dignity. In an era, where technology surrounds every facet of life, the potential for data misuse or mishandling is no longer a rare occasion, making such protection more crucial than ever. The enactment of Digital Personal Data Protection Act marked a major step towards strengthening individual privacy rights. Likewise, other countries have also taken initiatives to protect privacy of their citizens by implementing robust frameworks. This paper examines the provisions of Digital Personal Data Protection (DPDP) Act and attempts to compare it with the General Data Protection Regulation (GDPR) which majorly governs data protection laws in European Union.

Keywords: GDPR, DPDP Act, Data Protection, K.S. Puttaswamy, Privacy

INTRODUCTION:

Data in simple terms can be defined as a "piece of information". When this related to an information which is unique to an individual and basis on which an individual can be identified, such information can be called as "personal data". With rapid increase in the growth of technology

[1] *Author is employed as an in-house counsel in a fintech company*

and the consequent digitalization of our life, data has become one of the most crucial assets in today's world. Even for our basic day-to-day tasks such as buying groceries or booking cabs, we are required to provide personal details such as name, residential address, contact number, bank details etc. Also, people's increased involvement on social media platform, considering that such details are sensitive and unique to an individual, and the rising incidents of data breach, it is important to adopt strong measures to check against the incidents of data breach and misuse of data. Data breach can be understood as when there is an unauthorized access to sensitive information. Data Breach can happen either intentionally or accidentally. In 2023, a report issued by Mint, Resecurity, a US-based cybersecurity firm claimed that personal information of about 81.5 crore Indians has been leaked on the dark web. Such information consisted of names, phone numbers, addresses, Aadhaar, and passport information. Facebook suffered a major data breach in March 2021, when 533 million user records such as full names, phone numbers, user locations, biographical information, from 106 countries were posted on a hacking website. Another such incident being the data leak of Dominos India which occurred in May 2021, in which massive data of customers of Dominos India was leaked and was easily accessible in public domain. Cambridge Analytical Facebook Data Scandal which occurred in 2018, is one of the other incidents which inflicted a significant blow to the privacy of individuals. A brief account of the incident is that Cambridge Analytica was a political consulting firm which claimed to work on data-driven political campaigns. It used a third-party app called "This Is Your Digital life" to get access to data of Facebook users. According to the reports, users were paid to take a psychological test and via this, the app collected data. This was not only limited to people participating in the quiz, but also to user's Facebook friends. Whistleblower Christopher Wylie revealed that the data obtained by Cambridge Analytica was used to develop "psychographic" profiles of people and then, pro-Trump materials were delivered to them online. In this way, people were influenced in their choices.

The digitalization of our life has increased the risk of privacy infringement and in most of the cases, people are not even aware that misuse of their personal data is done. Most of the websites and applications often employ cookies or other tracking mechanisms, without explicit consent of the user and the user might not even have clear understanding of it. Additionally, some websites do not allow user (or visitor) to proceed unless they agree to accept all cookies.

To effectively address the threats of data breach, it is required that a robust framework must be created. As per data shared by United Nations Trade and Development (UNCTAD) in 2021, about

71% of the world's countries have a legislation towards Data Protection and Privacy Legislation and 9% of the countries have draft legislations prepared. 15% of the countries still have no legislations towards data protection. However, recently, this data was updated, showing almost 79% of UN member states have enacted data protection and privacy legislation as of July 2025. [2] This shows a surge in the earlier percentage, indicating that the majority countries now maintain regulatory framework for data protection. The first step was taken by Sweden when it enacted the first data privacy law. In 2016, the European Union adopted the General Data Protection Regulation (GDPR) which replaced the 1995 Data Protection Directive to keep pace with the rising advancement of the internet. India also took an initiative when it amended Information Technology Act in 2008 and also enacted Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Further, in one of the landmark judgements of K.S. Puttaswamy vs Union of India, Right to Privacy was recognized as an intrinsic part of the right to life and liberty under Article 21 of the Constitution of India. The Hon'ble Supreme Court in its judgement held that *"Right to privacy is a fundamental right- it is a right which protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices- The technology has made it possible to enter a citizen's house without knocking at his/her door and this is equally possible both by the State and non-State actors- It is an individual's choice as to who enters his house, how he lives and in what relationship."* Recognizing right to privacy as a fundamental right is one of the major steps in assuring greater personal freedom and upholding dignity of an individual and thereby improving quality of human life.

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011:

Rule 3 of the Privacy Rules includes Sensitive personal data or information which shall include password, financial information (such as Bank Account or credit card or debit card or other payment instrument), physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information or any detail received by body corporates for providing service or for processing or storing such information under lawful contracts or

[2] *United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide, UNCTAD,* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

 ISSN: 2584-0649 (O)

otherwise. An exception has been provided to this, as any information which is freely available in public domain shall not be regarded as sensitive personal data or information.

Obligations on the Body Corporates:

1) A body corporate[3] which collects, receives, process, stores, deals or handle personal information to provide privacy policy which shall be published on its website. The privacy policy shall be clear and easily accessible and shall provide the type of personal or sensitive personal data or information collected, purpose for collecting and usage of such information, disclosure of such information and reasonable security practices provided.
2) A body corporate shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data. If the personal information is collected directly from the person, then the body corporate shall ensure that the person concerned is aware that his/her information is collected, the purpose for collection of the information, who are the intended recipients and name and address of the agency that is collecting the information and the agency retaining the information.
3) Sensitive information shall not be collected except for lawful purpose connected with a function or activity of the body corporate.
4) Retention of sensitive personal data or information shall not be beyond legal requirements.
5) Information collected shall be used for the purpose for which it has been collected.
6) Body corporate (including any person on its behalf) shall keep the data secure.
7) Any sensitive data or information shall not be published by a body corporate.

Withdrawal of Consent:

Prior to collection of the information (including sensitive personal data), a body corporate shall provide an option to the provider of the information to not to provide the data which is to be collected. Additionally, an option shall be provided to withdraw its earlier given consent.

The withdrawal of the consent shall be made in writing to the body corporate.

[3] *Explanation to Section 43A of Information Technology Act 2000 defines body corporates as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities"*

If the provider of the information is not providing or withdrawing his consent, then the body corporate shall have an option to not provide goods or services in respect of which information was sought.

Grievance Redressal:

Any discrepancies or grievances of provider of the information shall be addressed by the body corporates within a stipulated time. A Grievance Officer shall be appointed by the Body corporates and publish his name and contact details on its website.
Any grievances raised shall be resolved expeditiously and within a period of one month from the date of receipt of grievance.

Disclosure of Information: Any sensitive personal data or information shall be disclosed by the body corporate to any third party with the prior permission of the provider of such information unless he has agreed to such disclosure or if such disclosure is required to comply with a legal obligation.

However, no prior consent shall be obtained if disclosure of the information is to be made to Government agencies as provided under the law or is required for purpose of verification of identity or prevention, detection or investigation of any offences.

The Rules does not debarred transfer of sensitive personal data to other body corporate or any person in India or located in any other country. However, the country to which such data is transferred must have similar data protection laws as the one to which the body corporate adheres to.

Reasonable Security Practices and Procedures:

A body corporate shall implement security practices and standards (International Standard IS/ISO/IEC 27001) and have a comprehensive information security program and information security policies containing managerial, technical, operational and physical control measures that commensurate with the information assets.

In case there is a security breach, the body corporate shall demonstrate to the agency that adequate security measures were placed as per the documented information security program and policies.

 ISSN: 2584-0649 (O)

The Rules also mandated audit of reasonable security practices and procedures shall be done by an auditor at least once a year and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

Digital Personal Data Protection Act, 2023

The Act was passed to regulate processing of digital personal data to ensure that personal data of individuals are protected, and such data are processed for lawful purposes. The Act still awaits its implementation.

The Act introduces some important concepts such as Data Fiduciary, Data Principal, Consent Manager.

Consent Manager has been defined as a person[4] registered with the Board, and who enables a Data Principal to give, manage, review and withdraw her consent. Data Fiduciary is any person who alone or in conjunction with other persons determines the purpose and means of processing[5] of data.

Data Principal means an individual whose personal data has been collected. In certain cases, if such person (whom the data relates) is a child or a person with disability, then her lawful guardian shall also be included.

Data Processor signifies any person who processes personal data on behalf of a Data Fiduciary.

Section 3 provides that the Act applies to processing of digital personal data within the territory of India and data collected in digital form or collected in non-digital form and then digitized. Also, the Act applies to processing of digital personal data outside India, but such processing is to provide goods or services to Data Principals within the territory of India.

Under following circumstances, the Act shall not be applicable-

i) Where personal data has been processed for any personal or domestic purpose;

[4] *Section 2(s) of the Act provides that person includes – an individual, a Hindu undivided family, a company, a firm, an association of persons or body of individuals, whether incorporated or not, the State, artificial juristic person*

[5] *Includes collection, recording, organization, structuring, storage, adaption, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction*

ii) Personal data has been made publicly available by the Data Principal herself or any person who is legally obligated to make such data public.

Grounds on which data can be processed:

i) If the Data Principal has consented to it,
ii) For certain legitimate uses.

A notice shall be given to the Data Principal stating-

a) the purpose for which the Data is to be processed,
b) manner in which the Data Principal shall exercise her rights,
c) procedure for raising complaint to the Board.

The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous. The consent shall be clearly communicated with a clear affirmative action.

Rights available to Data Principal under the Act:

1) Right to give consent: If data pertaining to a Data Principal is required to be processed and the basis of such processing is on ground other than legitimate uses, then the Act has granted a right to give consent to Data Principal. The Data Principal can reject the request as proposed by the Data Fiduciary.
2) Right to access information about personal data: Data Principal shall seek following information from Data Fiduciary:
   a) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by the Data Fiduciary,
   b) identities of all Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, also a description of the personal data so shared and
   c) any other information related to the personal data of such Data Principal.

3) Right to correction and erasure of personal data: This includes the right to correction, completion, updating and erasure of her personal data for the processing of which she has given consent.

 ISSN: 2584-0649 (O)

4) Right to withdraw: If the consent is the basis of processing of data of a Data Principal, then she has a right to withdraw her consent at any time.
5) Right of grievance redressal: In case there is breach of any obligations with respect to personal data of Data Principal, she has a right of readily available means of grievance redressal to be provided by Data Fiduciary or Consent Manager.
6) Right to nominate: Data Principal shall have a right to nominate any other individual, who shall in the event of death or incapacity of the Data Principal shall exercise the rights of the Data Principal as provided under the Act.
7) Right to complain to the Board: The Act provides a Data Principal the right to make a complaint to the Data Protection Board of India in case of any personal data breach or breach committed by the Data Fiduciary of its obligations.

Along with rights, certain obligations have also been imposed on Data Principal:

a) Compliance with the law: A Data Principal must comply with the provisions under the Act.
b) No Impersonation: The Act bars Data Principal from impersonation of another person while providing her personal data.
c) Non-Suppression of information: A Data Principal shall not suppress any material information for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities.
d) Frivolous Grievance: A Data Principal shall not register a false or frivolous complaints with Data Fiduciary or the Board.
e) Authentic Information: Information furnished by Data Principal shall be verifiably authentic.

Obligations on Data Fiduciary:

a) Data Fiduciary shall ensure completeness, accuracy and consistency of data if the data processed is likely to be used to make a decision affecting Data Principal or is to be disclosed to another Data Fiduciary.
b) Implement appropriate technical and organizational measures for complying with the provisions of the Act.

c) Protect personal data in its possession or under its control (including data processed by a Data Processor on its behalf).
d) Intimate the Board and affected Data Principal in case of any breach.
e) Unless data retention is required, erase personal data of the Data Principal, in case she withdraws her consent. Also, ensure that Data Processor (processing data on its behalf) erases such data.
f) Publish contact details of the Data Protection Officer (if required to have one) who shall be responsible for answering on behalf of Data Fiduciary, all queries raised by the Data Principal in respect of processing of her personal data.
g) Establish means for grievance redressal.
h) In case of processing of personal data of children or a person with disability, Data Fiduciary shall obtain a verifiable consent of the parent or the lawful guardian.

Digital Personal Data Protection Act also introduces the concept of "Significant Data Fiduciary. A Data Fiduciary may be classified as a "Significant Data Fiduciary" based on following factors:

- Volume and sensitivity of personal data processed,
- Risk to the rights of Data Principal,
- Potential impact on the sovereignty and integrity of India,
- Risk to electoral democracy,
- Security of the State,
- Public Order

Significant Data Fiduciary has been obligated to appoint a Data Protection Officer. A Data Protection Officer shall-

a) Represent the Significant Data Fiduciary under the provisions of the Act,
b) Shall be based in India,
c) Be responsible to the Board of Directors or similar governing body of Data Fiduciary
d) Act as point of contact for the grievance redressal mechanism,
e) Appoint an independent Data Auditor to carry out data audit for evaluating the compliance of the Significant Data Fiduciary.
f) Initiate Data Protection Impact Assessment.

Exemptions provided under the Act for processing personal data of a Data Principal:

a) If processing of personal data is required for enforcing any legal right or claim;
b) When any court or tribunal or any other body entrusted with performing any judicial, quasi-judicial or regulatory or supervisory function and processing is necessary to carry out the functions;
c) Processing of personal data in furtherance of prevention, detection, investigation or prosecution of any offence or contravention of any law;
d) When data to be processed relates to Data Principals based not within the territory of India and such processing is pursuant to any contract entered into between any person outside the territory of India and person based in India;
e) Where processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger;
f) Processing of data is required for ascertaining the financial information and assets and liabilities of any person who has defaulted in payment of any loan or advance.

Additionally, the provisions under this Act shall not apply where processing of personal data is required by any instrumentality of State in the interests of sovereignty and integrity of India and for maintaining security of the State. Also, if processing of data is required for research, archiving or statistical purpose.

The Act also mandates the creation of a Data Protection Board to which incidents of data breaches shall be intimated to. The Board shall be responsible for providing remedies or mitigation measures and to inquire into such incidents.

General Data Protection Regulation (GDPR) is a comprehensive data protection law enacted by the European Union. It aims to provide individuals an enhanced control over their personal data and to provide a uniform framework for data protection laws across European Union. Article 1 of the GPDR states:

"The Regulation lays down rules relating to the protection of natural persons with regards to the processing of personal data and rules relating to the free movement of personal data"

It is one of the robust legislations in the world for ensuring data protection and safeguarding individual privacy.

Some of the similar provisions between General Data Protection Regulation (GDPR) and Digital Personal Data Protection Act (DPDPA):

One of the common grounds for processing of personal data is obtaining consent from Data Principal/Data Subject. Any data which is processed with the consent of a Data Principal/Data Subject shall be lawful. The term 'consent' has been defined in a similar manner under both Acts as free, specific, informed, unconditional, indication of the Data Subject/Data Principal's wishes of a clear affirmative action, and shall signify agreement to the processing of personal data relating to him or her.

Under GDPR and DPDP Act certain common set of rights have been provided to a Data Principal/Data Subject such as Right to access information, Right to erasure, Right to withdraw consent and Right to Rectification. These rights enable a Data Principal/ Data Subject to protect their interest and check against any unauthorized processing of personal data of Data Principal/Data Subject.

Some of the common obligations placed upon Data Fiduciary/Data Controller:

a) Implementation of appropriate technical measures to ensure that any processing of data is undertaken so that objective of data protection can be achieved.
b) Intimation to the concerned authority and affected Data Principal/Data Subject in case of a data breach.
c) Protecting personal data by Data Fiduciary/Data Controller which is under its control.

Additionally, both the Acts provides for Data Protection Impact Assessment. GDPR mandates those Data Controllers to conduct assessment whose processing of data poses high risk to the rights and freedoms of natural persons, DPDPA obligates only a particular class of Data Fiduciary (Significant Data Fiduciary) to carry impact assessment.

Both the GDPR and the DPDPA include provisions for the processing of children's data. Under the GDPR, the processing of the personal data of a child of 16 year old and above shall be lawful if the child has consented to processing of his/her personal data. For children less than 16 years, processing shall be lawful only when such processing is authorized by any person who hold a parental responsibility. The provision contained under DPDPA is more elaborate on this front, as it includes people with a disability also. For processing of personal data pertaining to a child,

consent of the parent or lawful guardian is a must. Any processing of data which is likely to be detrimental to the interest of a child shall be prevented.

Under GDPR, an exception has been carved out in Article 2 (2) (d) restricting the application of the Regulation to processing of data undertaken by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security. Similarly, under Section 17 (c) of DPDP Act, one of the exemptions provided are processing of personal data which is done in the interest of prevention, detection, investigation or prosecution of any offence or contravention, can be done without obtaining explicit consent of the Data Principal.

One of the grounds for lawful basis for processing of personal data under GDPR is when a processing is necessary for compliance with a legal obligation of Data Controller. A provision similar to this exists under DPDP Act where Data Fiduciary is required to process the personal data of a Data Principal to comply with any obligation under any law and also for complying with any judgement or decree or order issued under any law. Additionally, an exemption has been provided in case where personal data is processed by any court or tribunal or any other body performing judicial or quasi-judicial or regulatory or supervisory functions.

If processing of personal data is necessary to protect the vital interests of the Data Subject or another natural person, it is one of the lawful grounds for processing of personal data under GDPR. By inclusion the terms “vital interest”, GDPR has kept the scope wider. DPDPA also contains similar provision. A Data Fiduciary may process the personal data to respond to medical emergency pertaining to either Data Principal or any other individual.

Both GDPR and DPDPA provides that an agreement (known as Data Processing Agreement) shall be entered into between a Data Fiduciary/Data Subject and a Processor for processing of personal data of a Data Principal.

Both Acts mandate that, in the event of a personal breach, the relevant authorities along with shall be notified within a period of 72 hours. Also, an intimation shall be given to the Data Principal without undue delay.

Data Protection Officer (DPO):

Both DPDPA and GDPR include provisions for the appointment of Data Protection Officer. Under DPDPA, only a Significant Data Fiduciary is required to appoint a Data Protection Officer. Similarly, under GDPR, a Data Controller or a Processor must designate a DPO if-

a) the processing is carried out by a public authority or body, except if such processing is done by courts in their judicial capacity;
b) the controller or the processor is primarily engaged in processing activities and require regular and systematic monitoring of data subjects on a large scale;
c) the core activities of the controller or the processor involves processing of special categories of data and personal data relating to criminal convictions and offences.

Under GDPR and DPDPA, it has been mandated that consent requests directed to a Data Subject/Data Principal, shall be presented in a clear, concise and plain language to ensure transparency and informed decision-making.

Some of the differences between GDPR & DPDP Act:

As enshrined under Article 1 of GDPR, the regulation establishes provisions for protection of natural persons with respect to the processing of personal data and rules relating to the free movement of personal data. In contrast to this, DPDPA specifically governs the processing of personal data in digital form. From this, it can be inferred that the GDPR has a broader scope, as it applies to the processing of personal data in both digital and physical forms, whereas the DPDPA has a limited approach to regulating only digital personal data.

Under GDPR, personal data is categorized into different types such as genetic data, biometric data, and health data. Further, it prohibits the processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data which uniquely identifies a natural person. Also, data concerning health or a natural person's sex life or sexual orientation is also restricted. However, the DPDPA does not categorize personal data into special categories, nor does it explicitly prohibit the processing of sensitive data.

The concept of "Consent Manager" is unique to DPDPA. Consent Manager has been defined as a person who is registered with the Board, who shall act as a single point of contact to enable a Data

Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

Under Article 30 of GDPR, provides that both Data Controller and Processor are required to maintain detailed records of their processing activities. However, DPDPA doesn't explicitly puts an obligation on Data Fiduciary or Data Processor to keep records of data processed by them.

DPDPA provides all Data Principal, right to nominate by virtue of which, he/she will have the right to nominate any other individual, who shall in the event of death or incapacity of the Data Principal, be responsible for exercising rights of the Data Principal. GDPR does not provide an explicit right to nominate another individual to exercise a Data Subject's rights on their behalf.

Under the DPDPA, the right to grievance redressal is explicitly recognized as one of the rights available to a Data Principal. In the event of any breach or failure by the Data Fiduciary to fulfil its obligations under the Act, the Data Principal must be provided with means of grievance redressal by the Data Fiduciary or the Consent Manager. Although, GDPR, does provide mechanisms for lodging complaints with supervisory authorities and seeking judicial remedies, it does not explicitly enumerate 'right to grievance redressal' as one of the core rights granted to a Data Subject.

One of the unique rights conferred by the GDPR upon a Data Subject is the 'Right to Data Portability' by which a Data Subject shall have a right to receive the personal data (belonging to him/her) which has been provided to a controller and have the right to transmit it to another controller without any hindrance from the controller. Provided that such processing is based on the consent of the Data Subject and is carried by automated means. No corresponding right has been provided under the DPDPA.

Provisions related to Cross Border Data Transfers:

Both the legislations aim to protect personal data of its citizens within and even when it is transferred outside their respective jurisdictions. While GDPR provides more elaborate provisions, DPDPA addresses this aspect briefly. Under GDPR, transfer of personal data is permitted to a third country or an international organization only if the Commission has sufficient reason to believe that such country or organization holds adequate level of protection. The Regulation lays down certain criteria for assessing an 'adequate level of protection' for the purpose of data transfer. The

Commission after assessing the adequacy of the level of protection, may determine whether a third country or international organization ensures adequate level of protection or not. In the absence of a decision, a controller or processor may transfer personal data by providing appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Some of the ways in which the safeguard can be provided by:

A) a legally binding and enforceable instrument between public authorities or bodies;
B) binding corporate rules are contained in accordance with Article 47;
C) standard data protection clauses adopted by the Commission;
D) standard data protection clauses approved by the Commission;
E) approved code of conduct, accompanied by binding and enforceable commitments from the data controller or data processor in the third country to apply appropriate safeguard;
F) an approved certification mechanism.

Even if any transfer of data is required to any jurisdiction outside European Union, a Data Controller or Data Processor shall not transfer such personal data unless there exists any international agreement or treaty for transfer. Such transfer must be justified on the grounds provided under the Regulation.

In contrast to such elaborate framework laid by GDPR for cross-border transfer of data, DPDPA briefly touches this arena. The Act lays down that the Central Government shall have a right to restrict transfer of personal data by a Data Fiduciary to any country or territory outside India. In the absence of such a restriction, the transfer of personal data may be permitted to different jurisdictions. This raises concerns about the potential risks of data breach and misuse of personal data of individuals.

Recently, on 23rd April, 2025, the European Data Protection Supervisor (EDPS), rejected the request of the European Investment Bank to transfer data such as contact details to other countries including India. The basis for this decision was lack of “adequate level of protection”. A clarification was also provided by the EDPS that this act of withholding the permission was not any verdict on India’s Digital Personal Data Protection Act. Instead, this decision was based on the lack of necessary justification of the required legal safeguards by the European Investment Bank. This triggers a very important discussion as to whether the DPDP Act will meet the adequacy standards required under the GDPR for cross-border transfer of data.

Penalty Structure under GDPR and DPDP Act:

Both the legislations impose stringent penalties in case of any violations committed. The penalties are imposed on a "tier basis" depending upon the nature and seriousness of the violations under both the Acts. The maximum penalty which can be imposed under GDPR amounts to €20 million or in case of an undertaking, up to 4% of the total worldwide turnover of the preceding financial year whichever is higher. Under DPDPA, maximum penalty which can be imposed is ₹250 crores and no turnover slab is taken into consideration while imposition of fines.

Some of the biggest fines imposed under GDPR was in 2023, when the Irish Data Protection Commission imposed a fine of €1.2 billion on Meta, taking a major step taken towards enforcement of data protection. The penalty was imposed on Meta for transferring personal data of European users to the United States without adequate data protection mechanisms. Another instance where such hefty fine was imposed was on Amazon in 2021. The Luxembourg National Commission for Data Protection ordered a fine of €746 million on Amazon, based on a complaint filed by 10,000 people, alleging that processing of data of the customers without proper consent. An investigation was taken and it was found that Amazon was in violation of the provisions as set out by the Regulation.

As the DPDPA, awaits its enforcement, there exists no instances of fines or penalties imposed for non-compliance under the Act, unlike the GDPR which has several enforcement actions for data protection violations.

CONCLUSION:

Data has become one of the most valuable assets in the today's digital world. Companies across different industries increasingly rely on data to drive growth and enhance their operations. However, thus data-driven expansion, comes at the cost of individual privacy. Often personal data of individuals including contact details, preferences, behavioural patterns are shared with third parties without the individual's knowledge and explicit consent. Such collection, sharing and processing of data are often promoted in the name of enhancement of experience, marketing purposes etc leading to large scale data harvesting. Personal data such as contact numbers, email address are frequently shared or sold to third parties without consent, leading to unsolicited messages, promotional calls, phishing and in some cases, offenders may use these to impersonate bank or government officials and extract sensitive financial information from a person. Images

uploaded on social media or stored in cloud apps, or picture editing apps, if shared and be morphed and used without consent. Data breaches whether accidental or intentional can lead to compromised personal data getting leak to the dark web or other unlawful platforms. Hence, to address these concerns, there is a need for a strong legal framework to prevent processing, sharing, storing of data without any legitimate ground.

While the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (commonly referred to as the SPDI Rules) laid down a regulatory framework for handling sensitive personal data such as obtaining consent, implementation of reasonable security practices, but had a limited effect in protection of personal data of individuals. In order to effectively address the rising digitization of personal data and potential risk of data protection, the Digital Personal Data Protection Act was passed. SPDI Rules extended protection to only sensitive personal data whereas DPDP Act facilitated protection to personal data including both sensitive and non-sensitive personal data, thereby expanding the scope. While SPDI rules are issued under Information Technology Act, 2000, DPDP Act is a distinct and comprehensive legislation. Further, SPDI puts obligations on the body corporate for ensuring protection while collection, storing, processing or handling of personal information. However, the DPDP Act has introduced a broader concept of Data Fiduciary to include any person who alone or in conjunction with other person determines the purpose and means of processing of personal data. One of the significant features of DPDP Act is emphasis on ‘consent’, as SPDI Rules only requires obtaining the consent and does without defining it as to when shall a consent be said to be a valid consent, but DPDP Act provides for obtaining clear, unambiguous, free, informed consent with a clear affirmative action. No set of rights are granted to a Data Principal (whom the personal data relates to) under the SPDI rules. Notably, SPDI restricts transfer of data by a body corporate to other body corporate or person in India or outside India unless there exists same level of protection adhered to by the body corporate under the Rules. As mentioned earlier, this provision has been modified as under DPDP Act only a transfer of data cannot be done if any restriction has been imposed by the Central Government. Under Section 43A of the Information Technology Act, a body corporate if held liable for any negligence for implementing reasonable security practises shall compensate the affected persons, implying that a compensatory model of penalty. DPDP Act provides for more stringent penalties for non-compliance. While the DPDP

Act draws its foundation from the SPDI Rules, it establishes a more detailed framework with robust mechanisms for regulating processing and also protection of personal data.

Both the General Data Protection Regulation (GDPR) and Digital Personal Data Protection (DPDP) Act aim to protect data protection and to regularize processing of personal data based on legitimate grounds. GDPR is a well-established legislation and has elaborate provisions for data protection while DPDPA is yet to come into effect. GDPR has set a high benchmark for data protection, inspiring data privacy laws in other countries and DPDP Act is one of them. The comparative study highlights that both legislations emphasize for lawful and transparent processing of personal data and puts an obligation on Data Fiduciary/Data Controller to adopt adequate security measures for ensuring data protection. The distinction helps to identify the gaps in one framework that may be addressed by adopting suitable provisions. In an increasingly interconnected world, the emergence of strong framework for data protection helps in building trust in digital world and providing greater control to individuals over their personal data. Both GDPR and DPDP Act have their own advantages and challenges, however timely and appropriate amendments in response to evolving needs will help these laws to better achieve their purpose.

***

REFERENCES

1. *K.S. Puttaswamy* v. *Union of India*, 10 SCC 1 (2017)

2. M. Komnenic *Top 10 biggest data breaches of all time*. Termly (Jan. 7, 2025) https://termly.io/resources/articles/biggest-data-breaches/

3. Jocelyn Fernandes, *Aadhar Data Leak: Personal Information of 81.5 Crore Indians on Dark Web: Top 7 Things to Know*, Livemint (Oct. 31, 2023) https://www.livemint.com/news/india/aadhaar-data-leak-personal-information-of-81-5-crore-indians-on-dark-web-top-7-things-to-know-11698737674480.html

4. Catherine Clifford, *Facebook-Cambridge Analytica Scandal: Everything You Need to Know*, CNBC (Mar. 21, 2018), https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html

5. Swathi Moorthy, *Why Is the Domino's India Breach Unusual and What Can You Do About It?,* Moneycontrol, (May 24, 2021), https://www.moneycontrol.com/news/business/why-is-the-dominos-india-data-breach-unusual-and-what-can-you-do-about-it-6931331.html

6. United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide, UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited on 26th July 2025)

7. Aihik Sur, *EU Data Watchdog Blocks EIB Data Transfer to India, Citing Privacy Concerns*, Moneycontrol, https://www.moneycontrol.com/technology/eu-data-watchdog-blocks-eib-data-transfer-to-india-citing-privacy-concerns-article-13014369.html#google_vignette (last visited on 29th July 2025)

8. Data Privacy Manager, *5 Biggest GDPR Fines So Far (2025*), https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ (last visited 29th July 2025)