INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Aug 2023
ISSN: 2582-6433

ASEAN OUTLOOK ON THE CONTOURS OF DATA PRIVACY LAWS: A SPECIAL EMPHASIS ON DIGITAL PERSONAL DATA PROTECTION ACT 2023

AUTHORED BY - PURANJAN PRASAD PAUL[1]

Abstract:

Data privacy is a contemporary concept that craves the attention of international as well as national fraternities owing to the rapid increase of technology, free flow of data and the handling of Data by multifarious intermediaries. In order to protect the privacy of individual data ASEAN Countries have taken a praiseworthy initiatives that eventually facilitates the vision of the assurance of Informational and Data Secrecy across the world. Compliance of key principles of Data Privacy should be adhered by the respective national legislations so as to fulfil the basic ethos of privacy. Cross Border Data Flow is another integral aspect that need special address in letters and spirit in order to protect the citizens data from any sort of exploitation.

KEY WORDS: *Data Protection, Data Privacy, Digital Personal Data Protection Act , Data minimisation.*

Introduction:

Information is the new commodity nowadays that can be sold out in lieu of money that attracts many prospective customers that can be used unfairly for felicitating the unfair purpose. In this parlance, data privacy is a necessary aspect that should be given due consideration. Before venturing into the core notions of Data Privacy it is necessary to replicate the concept of Right to Privacy at the international level and national level. Right to privacy is an important concept that gained its importance in the present era as it is an integral facet of Right to Life. Right to life does not imply the life with mere animal existence rather it signifies a fulfilled life that inculcates the concept of Privacy. [2]In order to attain the fulfilled life one should ensure the personal acts not to be disclosed informally with the third party. Right to privacy is a genus and Data Privacy is a specie that covers the spectrum of validating the privacy relating to data and information.

[1] Research Scholar , ICFAI Law School , ICFAI University Tripura , puranjanpaul@gmail.com, +918974861726
[2] Huggins, M. L. (2011). The Right to Privacy: An Argument for a Non-Derivative Right to Privacy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2416653

ISSN: 2582-6433

Right to Privacy is not an absolute term which is beyond any restrictions so owing to that Right to Privacy incorporates certain restrictions on the basis of which it can be curtailed[3] :

1. There is a legitimate state interest in restricting the right.
2. The restriction is necessary and proportionate to achieve the interest.
3. The restriction must have established by due procedure.

Concept of Data privacy

Data privacy, also known as information privacy, is a branch of data protection that ensures the confidentiality and immutability of sensitive data, including personal data, financial data, and intellectual property data, while meeting regulatory requirements. Data privacy, security, and backups are the three main data protection categories[4]. Best data security measures protect sensitive and personal data. Data privacy has many definitions. To put it another way, people (customers, employees, anyone) need to know what personal data firms are collecting about them and how they are using it. Data privacy laws introduce a number of new terms and concepts which are stated hereunder[5] :

'Data processing' or 'Processing'[6] means any automated or manual operation(s) carried out on personal data. In essence, this covers almost any relevant action word that could possibly be performed on information including collecting, recording, organizing, classifying, storing, modifying, amending, retrieving, using or revealing such data by broadcasting, publishing, transmitting, making available to others, integrating, blocking, deleting or destroying.

'Data protection authority' or 'Authority'[7] is the national body established to be responsible for upholding the rights of individuals to the protection of their personal data through the enforcement and monitoring of compliance with the local data privacy laws.

'Data Subject' or 'Individual' is defined as the person to whom the personal data relates. 'Personal data' is defined as information that relates to an identifiable person, either directly or indirectly.

[3] Yilma, K. M. (2015, May 24). Data privacy law and practice in Ethiopia. *International Data Privacy Law*, *5*(3), 177–189. https://doi.org/10.1093/idpl/ipv008
[4] OUTSOURCING: DATA SECURITY AND PRIVACY ISSUES IN INDIA. (2008). *Issues in Information Systems*. https://doi.org/10.48009/2_iis_2008_14-20
[5] Wong, R. (2013, October 16). Data Security Breaches and Privacy in Europe. Springer Science & Business Media.
[6] Gough, T. (1985, June). Data Processing Methods. *Data Processing*, *27*(5), 51. https://doi.org/10.1016/0011-684x(85)90145-5
[7] Dubey, R. K., & Verma, A. (2019, November 27). *Data Protection and Privacy Implementation*.

ISSN: 2582-6433

'Sensitive personal data' is a subset of personal data and is defined as information that directly or indirectly reveals a person's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to their health or sexual life.

Key Principles of Data Privacy

The key principles of maintaining and securing Data Privacy are labeled as the following stipulations[8]:

Lawfulness, fairness and transparency that implies one should always process personal data in a fair, lawful and transparent manner.

Purpose limitation implies that one should only process personal data for a specified and lawful purpose.

Data minimization signifies that one must ensure you are only processing the personal data that you truly need and nothing more. Integrity and confidentiality You must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.

Accountability signifies that one must have appropriate measures and records in place to be able to demonstrate your compliance.

In April 2017, ASEAN leaders issued a statement on cyber security cooperation, in addition to ongoing efforts such as the ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), the ASEAN Ministerial Conference on Cyber Security (AMCC), and the ASEAN Cyber Capacity Programme to foster regional cyber security cooperation (ACCP). Singapore has set aside S$10 million for the ACCP to improve technological capabilities among incident responders and operations in the region as a result of these platforms.

Data Privacy: Initiatives taken by South Asian Countries

The SAARC is made up of eight South Asian countries: India, Sri Lanka, Bangladesh, Pakistan, Bhutan, Nepal, Maldives, and Afghanistan. It is the developing hub for data privacy regulations; there is a good chance that South Asia will emerge with several laws that meet existing international standards9, but the indicators show that some countries are far ahead of others in terms of establishing privacy protection ethics in South Asia.

[8] Buyya, R., Calheiros, R. N., & Dastjerdi, A. V. (2016, June 7). *Big Data*. Morgan Kaufmann.
[9] Greenleaf, G. W. (2014, January 1). *Asian Data Privacy Laws*. Oxford University Press, USA.

ISSN: 2582-6433

Indonesia – The Ministry of Information and Communication Regulation No.20/2016 details more comprehensive regulation on Personal Data Protection. Law No. 11 of 2008 regarding Information and Electronic Transaction and Government Regulation No. 82 of 2012 regarding the Provision of Systems and Electronic Transactions ("PP 82/2012") has also been enhanced.

Malaysia – Malaysia is currently enforcing the Personal Data Protection Act 2010 (PDPA) through its Personal Data Protection Department.

Myanmar – In March 2017, Myanmar promulgated a 4-page law entitled Protecting the Privacy and Security of Citizens (Union Parliament Law 5/2017). According to the unofficial translation of the law7 by the Myanmar Center for Responsible Business (MCRB), the law explicitly prohibits interception of a citizen's electronic communications, private correspondences and, physical privacy, unless otherwise warranted by an "order".

Singapore – The Personal Data Protection Act 2012 (PDPA) has been in force since 2014, and is being implemented by the Personal Data Protection Commission.

Thailand – The Notification of the Electronic Transaction Committee on Policies and Practices for the Protection of Personal Information of Government Agencies BE 2553 (2010) and the Information Act for Public Sector BE 2540 (1997) protect its citizens' personal information that are being processed by state agencies. The Personal Data Protection Act is under development and expected to be published soon.

Philippines - The Data Privacy Act was passed in 2012, "to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth." This privacy law also established a National Privacy Commission to enforce and oversee it as well as giving it rule making power. Final implementation rules and regulations came into force in September 2016, given the Privacy Act specifically.[10]

Nepal

The right to privacy was initially included as a fundamental right in the Kingdom of Nepal's 1990 constitution, along with the right to information, and the right to privacy was later preserved in

[10] Greenleaf, G. (2018, January 1). 2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws - Trade and Human Rights Perspectives.

ISSN: 2582-6433

the interim constitution of 2007. However, there was no mention of the state's ability to hear complaints about infringement of private rights, although the public had the option of reporting such violations to the National Human Rights Commission (NHRC), as well as taking legal action in Nepalese courts. Nepal passed the Privacy Act of 2018, although it was not regarded a data privacy law because core principles were not included. Personal data gathered by business entities, for example, could only be used for the purpose for which it was collected, and collection and disclosure without authorisation were forbidden that affirms the need of obtaining consent before collecting private information, as well as the limitations on data collection and use for the purposes for which it was gathered.

India

The Aadhaar Card Scheme was challenged in this case on the grounds that gathering and compiling demographic and biometric information about citizens of the nation to be used for various purposes violates their fundamental right to privacy, which is personified in Article 21 of the Indian Constitution[11.]

At the same time, the Supreme Court was reviewing the evidence in the Retired Justice K. S. Puttaswamy (Retd) v. Union of India case12 , In order to examine the challenges surrounding data privacy, the Indian government established an expert committee in 2017 under the leadership of retired Supreme Court Justice B. N. Srikrishna. One year later, the committee presented a report and a bill draught. The current bill before the legislature is an altered version of the original draft of the bill.[13]

On December 11th, 2019, Minister of Electronics and Information Technology, made the first mention of personal data protection in the Lok Sabha. The Personal Data Protection Bill was intended to completely replace India's existing data protection system, which is now governed by the Information Technology Act, 2000 and the rules thereunder and was inspired by the GDPR14.The Bill outlines requirements for the processing and storage of personal data and outlines individuals' rights in relation to that data. To carry out this law, it seeks to establish the

[11] Arora, H. (2019). Grounds for Lawful Processing of Personal Data in GDPR and Personal Data Protection Bill 2018, India (PDPB): Section – I: Consent. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3718235
[12] GN, P. (2023). Justice K. S. Puttaswamy (RETD) VS. Union of India & ORS. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4468344
[13] N. (2020, February 12). Personal Data Protection Act of India (PDPA 2020): Be Aware, Be Ready and Be Compliant. Notion Press.
[14] Determann, L., & Gupta, C. (2018). Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3244203

ISSN: 2582-6433

Data Protection Authority, a new independent regulatory body in India. It will be necessary to collect and keep proof of the users' notification and consent. Consumers are also given the option to revoke their permission under the proposed legislation. Additionally, they are entitled to access, review, and deletion of their data. Corporations will need to set up procedures for obtaining consent from customers. Additionally, customers have the right to transfer to other companies their data and any conclusions that companies may have drawn from it. All companies will need to devise strategies to enable this for customers.

Impact of Digital Personal Data Act, 2023:

The Digital Personal Data Protection Bill of 2023 is a proposed legislation that aims to safeguard personal data in the digital realm. This Bill outlines key provisions and measures to protect individuals' privacy and ensure the secure handling of their personal information. It addresses concerns related to government and private entities' data collection, storage, processing, and sharing. This section's purpose is to thoroughly evaluate the Digital Personal Data Protection Bill 2022. The Bill has generated considerable attention and discussion as it tackles the increasing concerns about safeguarding personal data in the digital era. By conducting a thorough analysis of the critical provisions of the Bill, this evaluation seeks to provide insight into its potential consequences and efficacy in protecting individuals[15].The Digital Personal Data Protection Bill is currently undergoing a process of defining its boundaries. This is being done in response to a thorough evaluation of the potential impact of the Bill on privacy issues in India.

The Digital Personal Data Protection Bill, 2023 is a resonance of the Digital Personal Data Act that implies the following concerns:

- Employment should prioritise the principles of equity and transparency for the individuals involved in Nagriks.
- Data minimisation suggests that the collection of personal information should be restricted to only what is absolutely necessary to achieve a particular goal. The principle being discussed here is known as the principle of purpose limitation.
- The idea of accuracy in personal data suggests that it is essential to make careful efforts to maintain the correctness and up-to-date nature of an individual's personal information.
- The concept of storage restriction suggests that the continuous collection of Nagrik's personal information should not be considered permanent by default.

[15] Sundara, K., & Narendran, N. (2023, February 1). Protecting Digital Personal Data in India in 2023. *Computer Law Review International*, *24*(1), 9–16. https://doi.org/10.9785/cri-2023-240103

ISSN: 2582-6433

- Strict prohibitions should be imposed on acquiring and processing personal data that violates the law.
- The duration for which data is retained should be restricted to the necessary period needed to achieve the intended objective for which the data was collected. To ensure the successful achievement of the stated goal, it is imperative to implement logical and well-thought-out measures.
- The efficacy of data principles can be improved by implementing specific modifications, one of which is the introduction of post-mortem privacy measures.
- The proposed standards aim to give data principals the power to appoint a representative responsible for managing their data if they were to pass away or become unable to do so themselves.
- The facilitation of cross-border data transfer is an essential development in data governance, even though there is a strong emphasis on protecting data by storing it within India's jurisdiction.

While the Act has commendable attributes, it is crucial to recognise that certain elements could compromise data security even after implementation. "sensitive data" pertains to information of great importance to an individual, such as bank account numbers, date of birth, biometric information, sexual orientation, and more. The legislation before the Bill has already categorised specific data as sensitive. However, the Bill needs a well-defined framework for effectively handling and handling this sensitive data[16].

Furthermore, the Digital Personal Data Protection Act of 2023 has raised significant concerns :

- The first significant concern pertains to the Preamble of the Act, which highlights the inclusion of the right for individuals to safeguard their personal data and the lawful processing of such data. The language used in the preamble of the Act provides government agencies with a significant opportunity to restrict individuals' privacy rights. Including the phrase "matters connected in addition to that or incidental to it" in the preamble of the Act indicates that the government has the power to determine the legality of processing personal digital data without the consent of the data principal for a specific purpose.
- One of the main concerns is the lack of specific parameters that define Sensitive Digital Personal Data. However, the Act includes provisions for Significant Data Fiduciaries, which introduces additional obligations. The categorisation of Section 10 has focused on state

[16] Kemalasari, N. P. Y., & Putra, I. P. H. S. (2023, May 31). Protection of Medical Record Data as a Form of Legal Protection of Health Data through the Personal Data Protection Act. *Journal of Digital Law and Policy*, *2*(3), 111–118. https://doi.org/10.58982/jdlp.v2i3.338

ISSN: 2582-6433

intermediaries rather than Data Principals. The categorisation of Article 9 of the European Union GDPR is explicitly mentioned in this context.

- The absence of a comprehensive mechanism to regulate cross-border data flow is a significant concern. The user states that the provision for data flow outside of India is mentioned in The Present Act under section 16. They also say that the central government is responsible for handling this task and deciding which nations can have restricted access to personal data. In addition, it is worth noting that the Act does not explicitly exclude the adequacy rule outlined in Article 45-46 of the EU GDPR, which is used to determine the countries where data processing is permissible.
- The absence of specific provisions for Data Portability is a significant concern regarding Personal Data Privacy. Data Portability is essential as it enables individuals to change data fiduciaries easily. The protection of data principles is a necessary aspect of data protection.

In India, numerous laws and rules have been put out that mandate that particular categories of data be kept on servers. This includes the draught Personal Data Protection Bill, Reserve Bank of India notifications for 2019, the draught E-Pharmacy Regulations, and the report on non-personal data monitoring. The precedent-setting decision from August 24, 2017, is where the measure got its start. In that decision, the Supreme Court recognised privacy to be "a fundamental right" protected by the Indian Constitution. The Supreme Court requested that the government establish stringent data protection regulations on September 26, 2018.[17]

ASEAN Initiatives Regarding Cross Border Transfer of Data:

While ASEAN works to protect the data privacy of its more than 600 million population, the European Union, also sets out a similar regional arrangements by the implementation of General Data Protection Regulation (GDPR), which went into effect on May 25, 2018. The GDPR establishes a set of uniform data protection standards for the EU's 28 member countries, allowing citizens to understand how their personal information is used. The GDPR not only provides EU citizens control over their personal data, but it also makes the regulatory environment for multinational enterprises easier to navigate by consolidating EU regulations[18]. The distinction between the EU and ASEAN is that the EU has a parliament with legislative power, whereas ASEAN has the ASEAN Inter Parliamentary Assembly with persuasion power. Nonetheless, the

[17] Bakalis, C. (2017, October 30). Rethinking cyberhate laws. *Information & Communications Technology Law*, *27*(1), 86–110. https://doi.org/10.1080/13600834.2017.1393934
[18] Europe, C. O., & Rights, E. U. A. F. F. (2018, April 15). *Handbook on European data protection law*. Council of Europe.

ISSN: 2582-6433

GDPR is good news for ASEAN in terms of data and privacy protection in many aspects. Last year marked the 40th anniversary of ASEAN-EU relations. The EU is ASEAN's second largest commercial partner and largest source of foreign direct investment. The estimated seven million EU residents who go to ASEAN countries each year is the most significant[19]. Many ASEAN organisations would be compelled to comply with the GDPR as a result of this. In addition, the EU and ASEAN launched two flagship programmers in April 2018 on policy dialogue and regional economic integration with an overall budget of EUR 61 million to support the ASEAN integration process.

There is a narrow balance to be drawn between protecting personal data and erecting unneeded impediments of data flow. The imposition of severe restrictions on cross-border data transfers may stifle innovation. ASEAN formulated Model Contractual Clauses abbreviated as "MCC" for regulating the cross border Data Flows which are commercial terms and conditions that may be included in legally binding agreements between parties who exchange personal data across borders. The MCC's and their underlying obligations help parties to ensure that personal data is transferred in a way that complies with ASEAN Member States' (AMS) legal and regulatory requirements, protects Data Subjects' data which is based on the principles of the ASEAN Framework on Personal Data Protection (2016), and fosters citizen trust in the ASEAN digital ecosystem[20]. The MCCs are templates that outline the parties' responsibilities, as well as the necessary personal data protection procedures and related obligations. The MCCs were established in order to identify major difficulties for parties when transferring personal data across borders. The Asia Pacific Economic Corporation adopted a privacy guideline that all APEC members adhere to.

Conclusion

The above discussion highlights that South Asian countries have implemented significant measures to mitigate the risks of insufficient data privacy laws and regulations. The increasing dependence on digital tools in today's world has brought about unprecedented challenges posed by cybercriminals. The growing prevalence of cyber threats that extend beyond national boundaries has raised significant concerns among intelligence and security services. Addressing these risks has become an immediate and crucial focus, demanding urgent attention. The increasing prevalence of privacy threats has necessitated the search for solutions by institutions and government bodies. Prompt action is necessary to safeguard individuals and nations from

[19] Walters, R., Trakman, L., & Zeller, B. (2019, September 4). *Data Protection Law*. Springer Nature.
[20] Greenleaf, G. (2018, January 1). Privacy in South Asian (SAARC) States.

ISSN: 2582-6433

harm due to the insidious nature of cyber threats. These threats are characterised by the adversary's invisibility, difficulty in tracking, and potential lethality. The absence of a universally accepted framework for data protection is a significant gap on the global stage. The need for national data protection systems poses a substantial obstacle to the progress of regional data protection mechanisms. One possible solution to address this problem is for governments to thoroughly evaluate their existing national data protection procedures and make necessary improvements to enhance their effectiveness. The presence of well-defined protocols at the national level can promote productive dialogue to establish a cohesive and significant regional framework. The Digital Personal Data Protection Act 2023 is a highly anticipated legislation in India that is seen as a positive step towards protecting personal data. Certain areas necessitate a thorough examination by the legislature to ensure privacy protection for Indian citizens.