A TRANSATLANTIC COMPARISON: HOW THE DPDPA STACKS UP AGAINST THE GDPR

Grandhi Rohith, B.B.A. LL.B. (Hons), Sastra Deemed to be University

1. ABSTRACT

The old data protection rules that are existing and enforcing in India are being replaced by the Digital Personal Data Protection Act 2023. The Landmark Judgement of Justice K.S Puttuswamy (retd.) & Anr. v Union of India ((2017) 10 SSC 1)[1], popularly known as the Aadhaar case in which the supreme court of India recognised privacy as a fundamental right and highlighted to enact dedicated private legislation in the Country[2].

This New act in data Protection lays out guidelines for the fair, transparent, and legal processing of personal information. Additionally, it mandates that personal information be gathered only when necessary and kept for the shortest amount of time. This law in India strikes a compromise between the need to process personal data for legitimate purposes and an individual's rights to have it protected. The goal of these international initiatives is to strike a balance between encouraging innovation and economic growth and safeguarding people's privacy and control over their personal information[3]. This legislation seeks to achieve a balance between an individual's right to control and safeguard their personal data and the acknowledged necessity to process it for a variety of purposes. Coming up with a cure for a disease is not an easy task, especially when a term like privacy is dynamic and its interpretation also varies with the progression of society.

The Information Technology Act of 2000, which governs privacy matters in India, is already in place, however it does not fully handle the current status of data protection challenges. Since there is a significant advancement in the technology and regulation of electronic transactions but has lost some of its effectiveness in protecting people's Data privacy in today's society.

This study critically examines the scope, impact of implementing and

[1] Justice K.S Puttuswamy (retd.) & Anr. v Union of India ((2017) 10 SSC 1)

[2] Banerjee, S., & Tiwari, P. (2024, July 31). *Data Protection Laws and Regulations India 2024*. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/data-protection-laws-and-regulations/india

[3] Manupatra. (n.d.). *Articles – Manupatra*. https://articles.manupatra.com/article-details/A-Paradigm-Shift-In-Data-Protection-Analyzing-The-Digital-Personal-Data-Protection-Bill-In-The-Context-Of-India-s-Privacy-Landscape

broader objectives of this act. Furthermore, we will talk about how this act complies with the EU's GDPR.

Keywords: Digital Privacy, Data Protection, Personal Information, DPDPA, GDPR, PDPA, CCPA.

2. Introduction:

The DPDP Act, which aims to safeguard the privacy of personal data belonging to Indian citizens. It is the nation's first comprehensive legislation towards the protection of personal data of the Individuals. The Data Protection Bill, which was tabled in parliament in 2019 and underwent numerous revisions before being adopted by both houses of Parliament in 2023 and entering into force in 2024, served as the model for the DPDP Act. Because of societal improvements, the DPDP act of 2023 was proposed to replace the current data and technology laws. The law outlines the responsibilities and rights of data fiduciaries as well as data principals.

In addition, it creates a new class of data fiduciaries called large data fiduciaries and sets punishments for data breaches. The DPDP Act recognizes verifiable consent for children and individuals with disabilities.

Any type of information or material that is processed or stored within a computer system or computer network is referred to as Digital data. Given our deep dive into the digital world, dedicated regulation on personal data alone is sufficient proof of the type of power it currently possesses.

A Data Fiduciary may process a Data Principal's personal data under Section 7 of the Act for a number of reasons, including when the Data Principal has voluntarily provided their data to the Data Fiduciary for a specific purpose without giving their express consent, as well as other purposes specified in the section.[4]

2.1. Objectives of the DPDP Act of 2023

The DPDP Act of 2023 is all about putting the power back in the hands of Indian nationals when it comes to their personal information. It's designed to keep our data safe and sound,

[4] Digital personal Data Protection Act, 2023, & 7, No.22, Acts of parliament, 2023 (India)

ensuring that companies handle it responsibly. With this act, individuals can take charge of their own information, deciding who gets to see it and how it's used. Plus, it's not just about privacy; the act also aims to spark economic innovation and growth, creating a more secure environment for businesses to thrive while respecting people's rights. Overall, it's a step in the right direction for both personal security and economic progress.

Regardless of whether an organization is based in India or not, this legislation applies to all organizations that handle the personal data of individuals residing in India.

2.1.1. Safeguard the Confidentiality of personal information belonging to Indian National:

The technology is growing rapidly in society and making things easier to access. The growth or advancements in technology are also having few drawbacks that are being advantageous to certain individuals who were breaching the personal information of others without consent. This issue was addressed by the DPDP act of 2023 that In order for the Data Principal to exercise her rights under the provisions of this Act, "all requests for consent under the provisions of this Act or the rules made thereunder shall be presented to her in a clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution, and the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal.[5]

2.1.2 Encourage appropriate Handling of personal information:

This legislation aims to safeguard the people's personal information with appropriate guidelines and ensuring the use of any personal information with consent of the individual. Making the privacy notes available and accessible in English and 22 other languages that were listed under 8th Schedule of Indian constitution. It Limits the Collection of data to what is required for the specific purpose of processing. This objective of the legislation is to prevent the misuse of personal information of the individuals and promote the usage of it only for certain purposes with the consent of the individual.

[5] Team, N. I. C. A. (2025, January 6). MEITY releases Draft Digital Personal Data Protection Rules, 2025 - Current Affairs. *Current Affairs - NEXT IAS*. https://www.nextias.com/ca/current-affairs/06-01-2025/meity-draft-digital-personal-data-protection-rules-2025

2.1.3. Give people the power to take control of their personal information:

The highlight part of this legislation is that even prohibits the state to access the personal information of individual even if there is a threat to national security. The DPDP act of 2023 also allows the people for transferring the data outside India except to countries notified by the central government.

2.1.4. Economic innovation and economic Expansion:

The Data Act seeks to preserve people's control over their data, increase the economic value of data, foster innovation, and support equitable access to and use of data.[6]

2.2 Key provisions of DPDP Act of 2023:

Some intriguing changes to the way our personal data is managed are brought about by the DPDP Act of 2023. First of all, it grants us, the people, a number of rights. We have the right to view our personal information at any time, request that it be deleted, and even protest if someone tries to access it without our consent. Conversely, businesses that manage our data—known as data processors and fiduciaries—have some significant responsibilities. To protect personal information, they must put strong security measures in place and notify the Data Protection Authority of India (DPAI) of any data breaches. Furthermore, the legislation ensures that we be aware of the use and status of our data. Organizations who violate the regulations risk heavy fines of up to 5% of their annual turnover or 500 crores, whichever is more. Overall, it's a big step toward protecting our privacy.

3. INTERNATIONAL LEGISLATIONS ON PERSONAL DATA PROTECTION

3.1. GDPR:

A regulation pertaining to data protection and privacy in the European Union (EU) and the European Economic Area (EEA) is known as the **General Data Protection Regulation (GDPR)**. The GDPR's primary goals are to restore people' and residents' control over their personal data and, by harmonizing EU regulations, to streamline the regulatory landscape for

[6] *The EU Data Act: What does it mean for you? | Deloitte Luxembourg | Technology*. (2024, February 23). Deloitte. https://www.deloitte.com/lu/en/Industries/technology/perspectives/the-eu-data-act-what-does-it-mean-for-you.html

global trade.

The most robust collection of data protection laws in the world is the General Data Protection Regulation, or GDPR[7]. These extensive data privacy and protection laws were introduced by the European Union and went into effect on May 25, 2018. The law gives people more control over their personal data and establishes strict guidelines for how any organization, inside or outside the EU, gathers, uses, and protects personal data.

3.1.2. Objectives of GDPR:

To prevent unwanted access, misuse, or even destruction, it is crucial to protect personal information. It all comes down to making sure that people's information is managed appropriately. Simultaneously, by consolidating different EU legislation, the regulatory environment for foreign company can be made much simpler. As a result, companies may concentrate more on expansion and less on following intricate regulations. Furthermore, giving citizens and residents back control over their personal data is revolutionary because it gives people the ability to manage their own data and prioritizes privacy in our digital lives. The overall goal of these actions is to make the environment safer and easier to use for all parties.

Regardless of the organization's location, the GDPR is applicable to all entities that handle the personal data of people residing in the EU.

3.1.3 Key provisions of GDPR:

A Data Protection Impact Assessment should be conducted before beginning any new project that can endanger someone's personal information. This stage assists in spotting any possible problems before they become serious ones. Next, you must have a good legal purpose for processing personal data if you are a data controller. One popular one is "legitimate interest," which essentially indicates that you have a valid purpose for what you're doing. Organizations must promptly notify the impacted individuals in the event that personal data is compromised, whether as a result of a cyberattack, an unforeseen calamity, or a human error.

people are entitled to easily accessible personal data, which makes it simple for them to transfer their information to another organization if they so desire. It all comes down to keeping things

[7] DryvIQ. (2022, October 3). *Data Privacy Regulation | DryvIQ*. https://dryviq.com/data-privacy-regulation

simple and safe for all parties.

3.2 PDPA:

In order to secure personal data in Singapore, the Personal Data Protection Act (PDPA) was created in 2012. The PDPA got amended recently to keep up pace with the European Union's GDPR in 2020 **(Personal Data Protection Amendment Act 2020)**. It is a supplement to sector-specific laws and regulations including the Insurance Act and the Banking Act.

3.2.1 Objectives of PDPA:

In the current digital era, protecting personal information is crucial. Your personal information should only be gathered, used, and shared by organizations when it is absolutely required and justified. This implies that they shouldn't be collecting your information purely for amusement or without a good reason. It all comes down to protecting your privacy and making sure that no one else is using your data. Therefore, the next time you are requested for your information, keep in mind that it is perfectly acceptable to wonder if it is truly necessary.

3.2.2 Key provisions of PDPA:

It's crucial to follow a few fundamental guidelines while managing personal data. First and foremost, personal information should only be used or shared for the purposes for which it was originally intended. Make sure everyone is on board before collecting or using their information because consent is really important. Additionally, don't keep personal information longer than is required; just use it for valid business purposes, and when you're done, securely destroy it. Make that the degree of protection offered by external businesses you work with outside of Singapore satisfies the requirements set forth by the Singapore Personal Data Protection Act (PDPA).

Additionally, it is important to refrain from sending marketing messages to individuals who have registered for the **National Do Not Call (DNC)** registry. Keeping these guidelines in mind helps build trust and ensures responsible handling of personal information.

3.3 CCPA:

The **California Consumer Protection Act of 2018** (CCPA) gives consumers more control over

the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law.

3.3.1 Objectives of CCPA:

The organization aims to enhance consumer protection by publishing safety alerts to inform customers about potentially harmful or risky products or services. It also provides guidance on consumer welfare initiatives to Central and State Government Ministries and Departments, ensuring a collaborative approach to safeguarding public interests. Additionally, it plays a pivotal role in establishing essential regulations to prevent unfair business practices and protect consumer rights, fostering a fair and transparent marketplace**.**

3.3.2 Key provisions of CCPA:

Consumers are empowered with several rights to safeguard their personal data and privacy in the digital age. The **Right to Be Informed** ensures individuals are aware of the personal data companies collect about them and understand how this data is processed and shared. The **Right to Opt-Out** allows consumers to refuse the sale or sharing of their personal information, providing greater control over their data. Through the **Right to Delete**, individuals can request that companies erase any personal data they hold about them and require service providers to do the same. Additionally, the **Right to Limit Use and Disclosure of Sensitive Personal Information** enables consumers to restrict companies from using sensitive data, such as social security numbers, bank account details, precise geolocation, or genetic information, except for specified purposes, such as fulfilling service requests. These rights collectively foster transparency, privacy, and accountability in data handling practices.

For several reasons, data protection is crucial. First of all, it is essential in preventing fraud and cybercrime, such as identity theft and those obnoxious phishing tactics that can ruin your life. Additionally, it protects our privacy and ensures that our individual rights are upheld. Furthermore, data protection is what enables organizations to comply with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Strong data protection also lowers reputational risks because no one wants to cope with the aftermath from a data breach.

Effective data protection guarantees that businesses can swiftly recover and easily repair their

systems in the event that something goes wrong and data is lost or destroyed. All things considered, protecting our data is crucial to our security and tranquillity.

4. **Historical background**:

The DPDP Act of 2023 is having its roots from the IT act of 2000. (Information and Technology Act of 2000) which was India's first formal step towards Cyber Security Laws.

4.1. Information and Technology Act of 2000:

The introduction of this act was due to rise of technology and electronic commerce over the past decades led to a surge in cybercrimes and data Offences in India. The National security was in great threat due to the advancements and increase in misuse of rising technology.

This act was the primary legislation in India that deals with Cybercrime and Electronic Commerce. IT act of 2000 was formulated to ensure the lawful conduct of digital transactions and reduction of cybercrimes on the Basis of the United Nations model law on electronic Commerce 1996 (UNCIRAL model)[8]. There are two schedules and thirteen chapters, totalling 94 parts in this act.

4.1.1. Importance of IT act 2000

The Information Technology Act, 2000, has been instrumental in fostering the growth of e-commerce and digital transactions in India by providing legal recognition to electronic records. It established the equivalence of electronic signatures to physical signatures, thereby enhancing the authenticity and legitimacy of digital documentation. To ensure the security and reliability of digital signatures and certificates, the Act introduced the Controller of Certifying Authorities (CCA), a government body responsible for their issuance and maintenance. Furthermore, it established the Cyber Appellate Tribunal, a specialized authority designed to handle appeals against decisions made by Adjudicating Officers under the Act, thereby strengthening the framework for resolving cyber-related disputes.

[8] Aklegalmantra. (2024, July 5). *IT Act 2000 | Information Technology*. Aklegalmantra. https://aklegalmantra.com/it-act-2000

4.1.2. Objectives of the IT Act 2000

We should concentrate on offering government services electronically and expediting digital transactions between companies and the general public in order to increase accessibility. This increases productivity in addition to saving time. At the same time, it's critical to enforce severe sanctions in order to combat cybercrimes such as identity theft and data theft. Everyone's peace of mind depends on a safe internet environment. Clear laws and guidelines that monitor online activity and digital communications must also be established. Positively, encouraging the expansion of the Indian IT and ITES sectors can stimulate entrepreneurship and innovation, resulting in a thriving tech environment that is advantageous to all.

4.1.3. Important sections of IT act of 2000

4.1.3.1 Section 43 of IT Act 2000:

It deals about various actions for which a penalty is imposed it done without permission from the person in charge of the system[9]. The actions are mentioned below:

- Access information from the system
- Download or copy data without proper authorisation
- Introduce virus or other malicious software into the system
- Cause damage to a computer network or database
- Stop an authorized user from using the system
- help others break the law
- Charge someone for services they haven't used
- Information that has been altered or removed in order to diminish its worth or create harm

[9] The Information and technology Act, 2000, & 43 No. 21, Acts of Parliament, 2000 (India)

- Take or alter the code that enables a computer program to function.

4.1.3.2 Section 66 of IT Act 2000

An individual will face consequences if they commit any of the acts listed in Section 43 with the purpose to commit dishonesty or fraud. This punishment can be up to three years in prison, a fine of up to Rs. 5 lakhs, or both, according to Section 66 of the IT Act 2000.[10]

4.1.3.3 Section 66A of IT Act 2000

To combat cases of cybercrime brought on by the development of technology and the internet, Section 66A was added to the Information Technology Act of 2000. Sending abusive messages via communication services is punishable under this provision.

According to this provision, the following situations will result in punishment:

- Sending content that is really offensive or intimidating.
- transmitting misleading information via a computer program or communication equipment with the intention of creating irritation, discomfort, danger, obstruction, insult, harm, criminal intimidation, animosity, hatred, or malice/
- sending any kind of communication or email with the goal of annoying, upsetting, misleading, or deceiving the receiver.[11]

4.1.3.4 Section 66B of IT act 2000

The penalties for dishonestly obtaining stolen computer resources or communication devices are described in Section 66B. According to this clause, anyone found in possession of a stolen computer resource or communication equipment faces a maximum sentence of three years in jail, a fine of up to one lakh rupees, or both.[12]

[10] The Information and technology Act, 2000, & 66 No. 21, Acts of Parliament, 2000 (India)
[11] The Information and technology Act, 2000, & 66A No. 21, Acts of Parliament, 2000 (India)
[12] The Information and technology Act, 2000, & 66B No. 21, Acts of Parliament, 2000 (India)

Penalties and Offenses Under IT Act of 2000[13]

Section	Offence	Penalty
Section 65	Tampering documents stored within a computer system	Imprisonment of 3 years or a fine of Rs. 2 lakhs or both
Section 66	Offences associated with computers or any act outlined in Section 43	Imprisonment of 3 years or a fine that extends to Rs. 5 lakhs or both
Section 66B	Dishonestly receiving a stolen computer source or device	Imprisonment for 3 years or a fine of Rs. 1 lakh or both
Section 66C	Identity theft	Imprisonment of 3 years or a fine of Rs. 1 lakh or both
Section 66D	Cheating by personation	Either imprisonment for 3 years or a fine of Rs. 1 lakh or both
Section 66E	Invading privacy	Either imprisonment up to 3 years or a fine of Rs. 2 lakhs or both
Section 66F	Cyber terrorism	Life imprisonment

[13] Acharya, M. (2024, April 17). IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties. Cleartax. https://cleartax.in/s/it-act-2000

5. Literature Review:

5.1. A Paradigm Shift in Data Protection: Analyzing the Digital Personal Data Protection Bill in The Context of India's Privacy Landscape

The article analyzes the Digital Personal Data Protection Bill within India's privacy framework. It explores key provisions like data minimization, purpose limitation, and consent-based processing, addressing compliance and enforcement challenges. The discussion emphasizes its transformative impact on India's digital ecosystem while contextualizing it globally.

5.2. GDPR vs. India's DPDPA: Analyzing the Data Protection Bill and Indian Data Protection Landscape

The article compares the EU's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (DPDPA). Both laws emphasize individual rights over personal data and impose obligations on organizations to ensure data security. Key differences include GDPR's stricter cross-border data transfer rules and classification of sensitive data, while DPDPA provides more uniform regulations. The piece also discusses compliance challenges for businesses operating in both regions.

6. COMPARING DPDP ACT 2023 WITH GDPR

6.1. Similarities between DPDP and GDPR

6.1.1. Exclusion of Anonymized Data:

In order to ensure that reidentification is impossible, techniques such as mathematical and technical factors must be used to sufficiently and irrevocably distort data.

While not specifically stated, the Digital Personal Data Protection Act 2023 implies that it will not apply to anonymized data, just like GDPR's Recital 26 states that it does not apply to anonymised data because it does not.

6.1.2. Consent:

A key component of both the GDPR and the DPDP Act of 2023 is consent. Both the DPDP Act and the GDPR mandate that data fiduciaries obtain the data principals' free, express, and

informed consent before processing their personal data, making sure that the processing serves a valid purpose.

Additionally, the Act mandates that the data fiduciary's consent request be given in multiple languages at the data principal's choice.

6.1.3. Data processing without consent:

Both the DPDP act and GDPR having consent as the key component even though the act still provides certain exceptions to data fiduciaries to access and process the personal data of the data principals without their consent for legitimate purposes[14].

Under Section 17 of the DPDP act of 2023 data fiduciaries got exceptional chances to access the personal data of the data principals during the case of medical emergencies, rendering any service or benefit to the data principal by the state or carrying out any duty imposed by law.

Section 17 of DPDP act is similar to GDPR which allows data fiduciaries to process the personal data of the individuals without their consent when it is necessary such as for a contract, legal obligations, vital interests, public authority, etc.

6.1.4. Data Protection Officer

Under section 10 of the DPDP act data fiduciaries are categorized into significant data fiduciaries which compels the data fiduciaries to appoint a data protection officer. They are responsible for the ensuring that the respective company is following regulations that are complying with data protection regulations.

This provision is also made under the section 37 of the GDPR although they are not limited to a certain class of data fiduciaries.

6.2. Differences between DPDP and GDPR

6.2.1. Categorization of data

[14] Mukhija, K., Jaiswal, S., Nirma University, Ahmedabad, India, & Nirma University, Ahmedabad, India. (2023). Digital Personal Data Protection Act 2023 in light of the European Union's GDPR. *Jus Corpus Law Journal*, 312–314.

GDPR categorises personal data into a separate subset namely special categories of personal data. However Digital personal data protection Act, 2023 does not provide such subsets. All personal information complies with the statute in a similar way.

6.2.2. Offline Data

Certain individuals store their data either in online or offline based on their interest. Section 3 of the DPDP act provides security only to the personal data of the data principals that is stored or available online but the GDPR ensures that all personal data of a data principal is protected even it is personal data of an individual that present offline rather than online.

6.2.3. Requirement for Notice

Notices to data principals are made compulsory under DPDP and GDPR. While under DPDP act any notice to the data principal must describe the reason for accessing the personal data, purpose, grievance redressal and consent withdrawal are only required to be given when the ground for the processing of personal data of the data principal by data fiduciary is consent.

These notices are to be provided under the regulation at the time or even before collection of personal data regardless of the ground for processing it. It also outlines a number of required features that must be included in such a privacy notice, such as the data protection officer's contact information, cross-border transfer information, retention duration, etc.

6.2.4. Data Breach Notification:

The Act requires that a data fiduciary notify the Data Protection Board and any impacted data principals of any personal data breach through a notice since data breaches pose a substantial hazard to the personal information of data principals. Although GDPR only requires such notifications in cases where the affected data principal is at significant risk, the Regulation also requires them.

7. Key Observations

The legislation, while acknowledging the rights of data principals, such as the right to be informed about data collection and access, does not provide adequate tools for effective enforcement. This limitation undermines the practical realization of these rights, as individuals

lack clear avenues to ensure compliance or address violations. Similarly, while the legislation grants the rights to access, rectification, and erasure of personal data, it offers insufficient guidance on how these rights can be practically exercised. The absence of a detailed framework for implementation creates uncertainty, leaving both individuals and organizations without clear directions to navigate such processes.

Furthermore, the Act empowers the Central Government to determine which countries or regions are eligible to receive data transfers, yet it fails to include transparent processes or criteria for these decisions. This lack of clarity introduces significant ambiguity, especially for businesses engaged in international operations. The uncertainty may lead to inconsistent decisions, which could disrupt cross-border data flows and hinder global business activities. As a result, the legislation's gaps in enforcement, implementation, and transparency present challenges that could limit its effectiveness in ensuring robust data protection and facilitating seamless international data exchange.

8. Recommendations

To enhance data protection and privacy, several measures can be implemented. Strengthening the consent mechanism is essential by providing clear and comprehensive guidelines for consent forms, ensuring they are understandable, transparent, and accessible to all individuals. Enhancing data localization requirements is another critical step to improve control, security, and privacy of data processed within India. This can be achieved by broadening the scope of data localization to encompass a wider range of data categories. Additionally, the development of comprehensive data breach notification protocols is necessary. Organizations handling data must be mandated to notify data principals and relevant authorities promptly in the event of a breach, with clear specifications regarding the timing and format of such notifications. These measures collectively aim to create a robust framework for data governance and security.

To strengthen the framework for data protection and privacy, several critical measures need to be introduced and implemented effectively. One of the foundational steps is to **strengthen the consent mechanism**. This involves providing clear and specific guidelines for designing consent forms, ensuring they are easy to understand, transparent, and accessible to everyone, including individuals with diverse literacy levels or disabilities. Consent forms should avoid technical jargon, provide clear explanations of how personal data will be used, and offer explicit options for granting or withholding consent. A robust consent mechanism ensures that

individuals can make informed decisions about their data and enhances trust in data-handling practices.

Enhancing data localization requirements is another vital measure to ensure the control, security, and privacy of data processed within India. By requiring that specific types of data be stored and processed domestically, organizations can mitigate risks associated with cross-border data transfers and ensure compliance with local laws. Expanding the scope of data localization to include additional data categories, such as sensitive personal data or financial information, can further strengthen national security and protect individuals' privacy. A well-defined framework for data localization will also encourage the development of local data infrastructure, contributing to the growth of the digital economy.

Additionally, the development of **comprehensive data breach notification protocols** is imperative for addressing incidents of data compromise effectively. Organizations must be mandated to notify data principals and the appropriate authorities immediately in the event of a data breach. This notification should adhere to clear standards regarding its timing, format, and content, providing detailed information about the nature of the breach, the data affected, and the steps being taken to mitigate the impact. Early notification enables individuals to take necessary precautions to protect themselves and ensures that regulatory authorities can respond promptly to contain the breach and enforce accountability.

Together, these measures—strengthened consent mechanisms, enhanced data localization, and robust breach notification protocols—lay the foundation for a comprehensive and secure data governance framework. By implementing these strategies, India can better protect individual privacy, ensure compliance with global data standards, and foster trust in its digital ecosystem.

This is to effectively handle the data breaches by the organizations and to ensure the safety to the data of the data principals.

9. Research Problem:

The DPDP Act in India has a different approach compared to the GDPR when it comes to the transfer of personal data to other countries. Here are the primary differences between the DPDP Act’s provisions and the GDPR restrictions on international data transfers:

9.1. Government-Approved Countries:

DPDP Act: According to the DPDP Act, cross-border data transfers are only allowed to nations or territories that the Indian government formally notifies as "trusted." This method centralizes decision-making and restricts data transfers to nations that have been authorized by the government.

GDPR: The GDPR depends on the European Commission's adequacy decisions, which evaluate and award "adequacy" status to certain nations according to their data protection policies and procedures. A thorough evaluation of the foreign nation's data protection regulations is required for GDPR's adequacy decisions, in contrast to the DPDP Act, which depends on government listings.

9.2. Use of Safeguards for Transfers:

DPDP Act: If a company wants to move data to a nation that is not on the government's approved list, the DPDP Act does not yet offer alternatives for protections (such as SCCs, BCRs, or certifications).

GDPR: When transferring data to nations without an adequacy determination, enterprises can utilize a number of extra transfer options that GDPR offers. These consist of Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs), and additional mechanisms such as certifications or codes of conduct. Because of this flexibility, enterprises can guarantee compliance even in nations where the degree of adequacy may not be acknowledged.

9.3. Derogations for Specific Situations:

DPDP Act: Derogations for data transfers to non-trusted countries, such as those for legal claims or contractual necessity, are not explicitly defined by the DPDP Act. As a result, in rare cases, businesses have few choices for moving data outside of authorized nations.

GDPR: GDPR contains special exceptions that allow data transfers in extraordinary circumstances, even in the absence of an adequacy ruling or other protections. These exceptions, which offer additional choices for legal transfers under particular circumstances, include express consent, contractual necessity, public interest, and legal claims.

9.4. Supplementary Measures and Transfer Impact Assessments:

DPDP Act: At the moment, the DPDP Act does not mandate the use of transfer impact assessments (TIAs) or supplemental measures when sending data to other nations.

GDPR: In response to recent court decisions (such as Schrems II), data exporters are required to perform transfer impact assessments (TIAs) to determine whether data in non-EU nations will be sufficiently protected, possibly necessitating the use of extra security measures (such as encryption or pseudonymization) when necessary.

9.5. Accountability and Documentation Requirements:

DPDP Act: Although it emphasizes more general data protection standards, the DPDP Act does not yet outline comprehensive documentation or accountability procedures for cross-border data transfers.

GDPR: GDPR enforces stringent accountability standards, such as keeping thorough records of data transfers and proving the need for them. Businesses must show that they are processing cross-border data in accordance with GDPR regulations.

9.6. Sector-Specific or Sensitive Data Considerations:

DPDP Act: The DPDP Act does not specifically classify or establish unique standards for sensitive data transfers; instead, it focuses on "digital personal data." Similar broad rules apply to all transfers of personal data.

GDPR: GDPR offers more safeguards for sensitive data (such as biometric or health information) and may impose more stringent requirements for sending such data abroad, particularly if the destination nation does not have sufficient protection.

10. Conclusion:

To meet the goals and objectives, the Digital Personal Data Protection Act 2023 could be improved to address a number of issues that have already been thoroughly discussed. To sum up, the Act represents a significant turning point in India's efforts to develop a comprehensive legal framework for protecting personal data and privacy. The effectiveness of

the legislation would be greatly increased by the aforementioned suggestions. Apart from safeguarding individuals' privacy rights, a well-crafted and equitable data protection law would promote creativity and confidence in the commercial sector and assist India in becoming a part of the global digital economy.

References:

1. A Paradigm Shift In Data Protection: Analyzing The Digital Personal Data Protection Bill In The Context Of India's Privacy Landscape Accessed on Nov 15 2024.

https://articles.manupatra.com/article-details/A-Paradigm-Shift-In-Data-Protection-Analyzing-The-Digital-Personal-Data-Protection-Bill-In-The-Context-Of-India-s-Privacy-Landscape

2. Data Protection Laws and Regulations India 2024. International Comparative Legal Guides International Business Reports. Accessed on Nov 13 2024.

https://iclg.com/practice-areas/data-protection-laws-and-regulations/india

3. GDPR vs. India's DPDPA: Analyzing the Data Protection Bill and Indian Data Protection Landscape. Accessed on Nov 12 2024.

https://secureprivacy.ai/blog/comparing-gdpr-dpdpa-data-protection-laws-eu-india

4. What is India's Digital Personal Data Protection (DPDP) Act? Rights, Responsibilities & Everything You Need to Know. Accessed on Nov 17 2024.

https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you

5. Digital Personal Data Protection Act, 2023: a Comprehensive Analysis. Accessed on Nov 16 2024.

https://blog.ipleaders.in/digital-personal-data-protection-act-2023-a-comprehensive-analysis/

6. Digital Personal Data Protection Act 2023 in light of the European Union’s GDPR

https://www.juscorpus.com/wp-content/uploads/2023/12/61.-Khilansha-Mukhija-Shreyas-Jaiswal.pdf