|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | |  |  |  | | --- | | **LexCognito**  ***This issue of LexCognito, which in Latin means 'awareness about law', seeks to provide you an insight into significant legal and regulatory developments that have taken place very recently in India.*** | | |  |  |  | | --- | --- | | |  | | --- | | **Date: 27 March 2024** | |  |  |  | | --- | --- | | |  | | --- | | **Comparison of India’s DPDP Act with EU GDPR** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | On August 11, 2023, the Indian Parliament passed the Digital Personal Data Protection Act 2023 **(“DPDP Act” or the “Act”)**, which is the country's first comprehensive data protection law. The DPDP Act is referred to as "umbrella" legislation since it just lays out the broad parameters for India's upcoming new data protection and data privacy laws and further regulations to implement the entire framework are anticipated down the road. Even though the new law is not yet in effect and the Government is expected to provide a reasonable breathing period to subjects (and corporates) to undertake adequate preparation since the law will warrant massive changes in IT systems, businesses who must comply with it are encouraged to start evaluating any potential practical ramifications as soon as possible.  Any processing of digital personal data in India will be subject to the DPDP Act. The law also has an extraterritorial impact since it covers the processing of digital personal data outside of India if it is related to providing goods or services to individuals within India who are referred to as "data principals". The DPDP Act outlines principles such as purpose limitation, data minimization, and accountability. It introduces the concept of significant data fiduciaries (**SDFs**), who bear heightened responsibilities, including appointing a Data Protection Officer (**DPO**). Cross-border data transfers, consent management, and breach reporting are key areas addressed by the Act.  One important European Union (**EU**) policy that sets forth detailed criteria for the gathering and use of personal data is the General Data Protection Regulation, **("GDPR").** Enacted in 2016 and coming into full force in May 2018, the GDPR affects companies globally that handle the data of EU individuals in addition to those operating within the EU. It presents the idea of Privacy by Design, putting a focus on proactive privacy issues during the creation and design of systems. The GDPR contains several key terminologies, such as controller, processor, data subject, processing, and personal data. The law gives people more power by giving them more say over how businesses manage and share their personal information.  The GDPR embodies the concept of Privacy by Design, emphasizing proactive privacy considerations during system design and development. Organizations must embed privacy principles into their processes, ensuring that data protection is integral from the outset. The regulation has far-reaching effects beyond the EU, impacting businesses worldwide. Entities supplying goods or services to the EU or monitoring EU citizens’ behaviour must adhere to GDPR requirements.  In summary, both the DPDP Act and the GDPR emphasize privacy, accountability, and data subject rights. Organizations operating in India or dealing with EU data must navigate these regulations meticulously to ensure lawful and ethical data handling practices.  **A COMPARISON OF GDPR AND DPDP ACT**  **(Issuance of Regulations/Rules Will Entail More Details)**   |  |  |  | | --- | --- | --- | | **Criteria** | **GDPR** | **DPDP Act** | | **Applicability** | The GDPR covers all organizations that process the personal data of EU citizens, including every company that offers goods and services or employs people in the EU even if an entity is based outside the EU. | Section 3 of the DPDP Act extends its scope to the processing of digital personal data within India where such data is:   1. collected online, or 2. collected offline and is digitised.   It will also apply to the processing of personal data outside India if it is for offering goods or services in India. | | **Categorisation of data fiduciaries/ data controllers** | The GDPR does not distinguish between classes of data controllers (equivalent to data fiduciaries under the DPDP Act). | The DPDP Act, 2023 has provided a further classification of data fiduciaries as SDFs based on a variety of items including the volume and nature of data collected. Pursuant to such governmental classification, additional obligations may be imposed on the notified SDFs. | | **Consent of minors** | The GDPR maintains the eligible age to provide consent at sixteen (16), but permits member states to reduce it to as low as thirteen (13). | Under section 2 (f) of DPDP Act, people under the age of eighteen (18) are considered minors and processing of their data requires verifiable parental consent pursuant to section 9 of the Act. | | **Consent managers** | There does not exist any concept in the GDPR regarding consent managers. | The DPDP Act lays down the concept of a ‘consent manager’ under section 2 (g) as a person registered with the Data Protection Board, who is accountable to the data principal and acts as a single point of contact to enable a data principal to manage their consents though accessible platforms. | | **Classification of data** | The GDPR classifies personal data into a further subset, namely special categories of personal data, which include data pertaining to racial or ethnic origin, political opinions, religious or philosophical beliefs etc. Special categories of personal data are subject to distinct compliance requirements. | The Act applies to the broader set of personal data, without further categorising it into sensitive or critical personal data and there exists no statutory requirement to implement separate compliance standards for different kinds of personal data. | | **Cross-border transfers of data** | The GDPR has laid down an exhaustive procedure for cross border flow of data. This is implemented through adequacy decisions, prescribed rules, standard contracts, and clauses relating to derogation. | As per the DPDP Act allows the Central Government to restrict the transfer of personal data by a data fiduciary to notified countries or territories outside of India, which shall be notified at a later stage. | | **Data breaches** | The GDPR requires reporting of personal data breaches to authorities. However, personal data breaches need to be intimated to affected data subjects only when such breaches are likely to result in high risk to their rights and freedom.   As per the GDPR, in regard to data breaches suffered by data processors, the data processors’ obligation is to only notify the concerned data controller of the same. The responsibility of reporting such personal data breach (if found to be meeting the necessary threshold set out under the GDPR) to the authority lies with the data controller. | The DPDP Act mandates both the data fiduciaries and the data processors to report personal data breaches and breach must be reported in all cases under the Act. | | **Data Protection Authorities** | The GDPR mandates establishment of supervisory authorities in each EU member state. | The DPDP Act stipulates the establishment of the Data Protection Board of India under section 18 of the Act, which would enforce regulations, enforce penalties, and resolve complaints. Key functions of the Board include:   1. monitoring compliance and imposing penalties; 2. directing data fiduciaries to take necessary measures in the event of a data breach; 3. hearing grievances made by affected persons; and 4. The Board shall conduct such inquiry following the principles of natural justice shall record reasons for its actions during the course of such inquiry. | | **Data retention period** | There is no prescribed retention period for data collected under the GDPR. It requires that entities retain data only until it is necessary for the purposes for which it was collected. | The DPDP Act follows a similar standard, but with a more prescriptive approach to deciding when a purpose is served. It specifies that if the user does not avail of the service for a period of time, or if they don’t exercise their rights for a period of time then the purpose will automatically be deemed to be served. For instance, if a user downloads an app and then does not use it for X number of months then the purpose will be considered fulfilled and the user data will have to be deleted. The government will define that this X period is through subsequent rules. | | **Notification to regulators** | Relevant data protection authorities should be notified without undue delay and not later than 72 hours after becoming aware of the breach, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. | In the event of a personal data breach, a data fiduciary is required to notify the Data Protection Board under the DPDP Act in the form and manner that will be prescribed through rules under the DPDP Act. Unlike the GPDR, the DPDP Act does not contain risk thresholds for the reporting of data breaches. | | **Obligations of data fiduciary** | Data fiduciary is responsible for strict levels of GDPR compliances. According to Article 24 of the GDPR, they must actively demonstrate full compliance with all data protection principles. | As per the section 4 of the DPDP Act, Data fiduciaries are responsible for:   1. Take consent for data processing activities; 2. Notify personal data breaches; 3. Apply technical safeguards and reasonable security measures; 4. Not to retain data beyond the restricted period; and 5. Appoint a grievance officer and DPO. | | **Penalties** | The GDPR prescribes fines under Article 83 and the same are administered according to the size of the organization, gravity and impact on non-compliance, and other criteria. As per the GDPR, penalties structure can be up to 20 million Euros or, in the case of an undertaking, up to 4% of the entire global revenue of the prior fiscal year, depending on what is higher, for very serious violations. Moreover, less serious violations can entail fines of up to 10 million Euros or, in the case of an undertaking, up to 2% of its total global revenue for the prior fiscal year, whichever is larger. | The DPDP Act prescribes an upper limit on the financial penalty for non-compliance and the same has been limited to not more than INR 2.5 billion under chapter VIII. Thus, the penalty can go up to INR 2.5 billion. | | **Processing of personal data** | The GDPR clearly mentions under Article 5 that lawfulness, fairness & transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity & confidentiality, and accountability shall be the core principles guiding the processing of personal data. | The DPDP Act has no express mention of any such principles in the Act itself. | | **Processing of personal data without consent** | The GDPR also enables data controller to process personal data without consent in specific situations while providing for certain obligations on the data controller. | The DPDP Act stipulates that under certain scenarios such as for performance of a state function, medical emergency, compliance with a decree or law etc., the requirement of consent can be overridden. This is referred to as legitimate uses under section 7 of the Act. | | **Right of data principals** | The GDPR outlines 8 fundamental rights, plus the right to withdraw consent, which guarantees individual autonomy over both personal data and its processing. These are mentioned below:   1. Right to be informed 2. Right to access 3. Right to rectify 4. Right to erasure 5. Right to data portability 6. Right to restrict processing 7. Right to object automated processing 8. Right to withdraw consent | Data principals have certain rights with respect to their personal data under chapter III of the Act:   1. Right to access 2. Right to correction or erasure 3. Right to nominate 4. Right of grievance redressal | | **Right of data portability** | The Right of data portability under the GDPR enables individuals to obtain and reuse their personal data for their own purposes across different services. | The DPDP Act does not provide the right of data portability in favour of data principals |     **\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*** | | | | | |