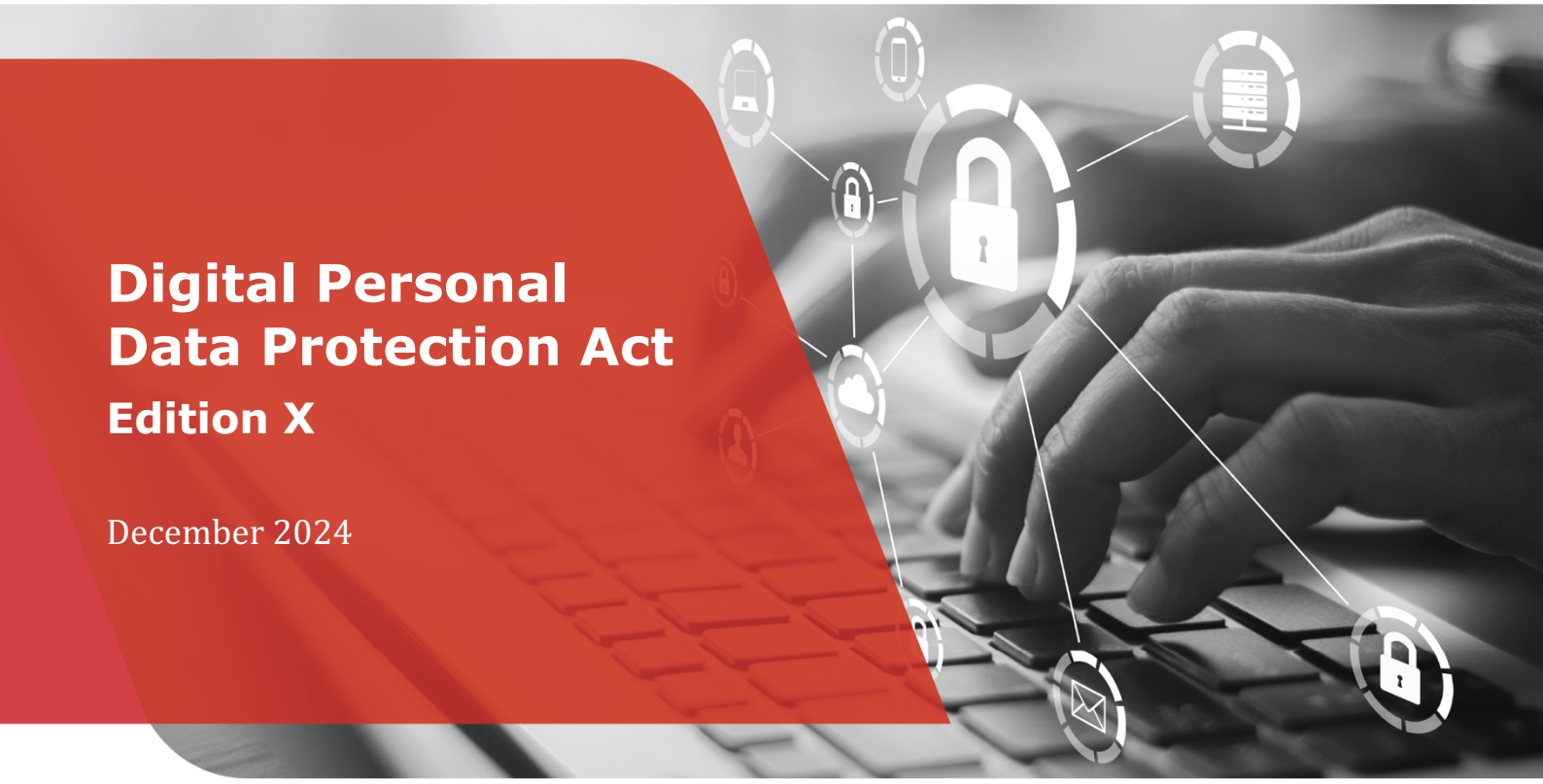
jsa
advocates & solicitors

JSA Prism

Privacy and Data Protection



Digital Personal Data Protection Act

Edition X

December 2024

Privacy and data protection in Artificial Intelligence

In the era of Artificial Intelligence ("**AI**"), the use of big data including personal data is considered to be indispensable in the training, development and deployment of AI systems. Personal data is leveraged at various stages, such as during the training of AI models, where vast datasets are processed to enable the AI model or system to identify patterns, and during the working of the AI system, where personal data may be continuously collected, analysed, and processed for the AI system to generate outputs. However, this extensive use of personal data raises significant privacy concerns, particularly regarding data protection, transparency, and accountability. In this edition of the Prism, we explore the intersection of AI and personal data, focusing on how specific provisions of the Digital Personal Data Protection Act, 2023 ("**DPDPA**") may apply to using personal data to develop, train, deploy or use AI systems.

Applicability of the DPDPA

An entity processing personal data for training, development or deployment of the AI models or system in India → needs to comply with the provisions of the DPDPA ← An entity outside India processing personal data for training, development or deployment of AI systems in connection with offering goods or services to data principals in India

In cases where entities outside India profile data principals located in India only for the purpose of training AI models, and the resulting systems are subsequently not made available in India, there could be enforcement issues as the DPDPA does not apply to processing of personal data outside India that is not in connection with offering goods or services to data principals in India.

Training on publicly available data

The DPDPA does not apply to the processing of personal data that has been made publicly available by the data principal themselves, or by any person who is legally mandated to make such data publicly available

The DPDPA exempts publicly available data from its scope, allowing unrestricted use for training Machine Learning/AI models, including through data scraping. Unlike Singapore's Personal Data Protection Act ("**PDPA**"), which maintains some safeguards, the DPDPA imposes no obligations if the data is made public by the data principal or through legal mandates. This contrasts sharply also with the European Union's General Data Protection Regulation ("**GDPR**"), which applies to all personal data, including public data. The European Data Protection Board's ChatGPT Taskforce has warned that scraping publicly available data, especially sensitive data, risks individual rights and requires safeguards to prevent misuse. The Belgian Data Protection Authority aligns with this perspective by requiring proportionality and data minimisation when personal data is processed.

In the United Kingdom, the Information Commissioner's Office highlights the need to adhere to GDPR principles even when processing publicly available data, stressing that such data is not exempt from privacy laws. This includes complying with lawful bases for processing, transparency, and ensuring data subjects' rights are protected

The ability to process publicly available personal data without any legislative oversight will give rise to 'invisible processing' where the data principals are not aware of the purpose for which their personal data is processed.

Where the AI model is trained on anonymised data, the DPDPA is not applicable as it does not qualify as 'personal data'.

Scraping publicly available data may not be covered under the DPDPA but could still result in other violations like breach of intellectual property rights, breach of contract, or unauthorised access under other applicable laws.

Legitimate uses for processing

Under the DPDPA, 'legitimate use' serves as a lawful basis for processing personal data without explicit consent, provided the processing aligns with certain specific, predefined purposes in the DPDPA. Legitimate use comprises processing for functions such as State operations, health emergencies, medical purposes, employment, and other uses listed under Section 7 of the DPDPA. The application of legitimate use, however, requires compliance with the principle of purpose limitation. It is common practice to repurpose personal data obtained for a primary purpose to train AI models. However, post the implementation of the DPDPA, the data fiduciaries will have to reassess the grounds for processing to either obtain specific consent to process personal data or rely on the legitimate use for training or working of AI models. Where AI is used to automate decision-making or make inferences about an individual, such processing may also generate new personal data. The data fiduciaries should ensure that they rely on a ground for the processing of this newly generated personal data as well.

AI in law enforcement and State functions

1. DPDPA allows the State or its instrumentalities to process personal data to provide or issue various benefits, services, or permits to data principals based, as a legitimate use. This enables the State and its instrumentalities to process citizen data to develop or deploy AI to augment administrative capacity. For example, states like Tamil Nadu, Telangana, and Andhra Pradesh are leveraging AI to improve public service delivery - such as water body management, pensioner authentication, and real-time beneficiary identification. These applications demonstrate how AI can not only streamline administrative functions but also create a more inclusive and responsive system of governance, reflecting a broader trend in AI-driven public services. The DPDPA does not create a bar on such use cases.
2. It is also, not uncommon for AI tools, particularly Automated Facial Recognition Technology (AFRT), to be integrated into law enforcement for tasks such as identifying criminals or locating missing persons. In some instances, AI is also used in predictive policing, helping authorities allocate resources effectively by predicting where crimes may occur. Similarly, AI applications are being tested for disaster management, ensuring the safety of citizens during calamities. However, such tools can facilitate constant monitoring of individuals in public spaces, posing risks to privacy rights, especially since, the processing of personal data in the interest of prevention, detection, investigation or prosecution of crimes or any contravention of any law in India is exempted from certain provisions of Chapter II of the DPDPA. Without proper policy or regulation, such surveillance can lead to an adverse effect on free expression and create an environment of pervasive monitoring.
3. Another significant concern is the potential for bias in AI systems. If AI models are trained on biased historical crime data, they may unintentionally reinforce existing prejudices. This can lead to discriminatory outcomes, such as unfairly targeting specific communities or perpetuating stereotypes. Furthermore, the lack of transparency in how AI algorithms process data can make it challenging to identify and address such biases, amplifying the risk of systemic inequities.

Processing of personal data belonging to children/persons with disabilities

If the training dataset contains personal data belonging to either children or persons with disabilities, or if an AI system processes such personal data, the data fiduciary must obtain verifiable consent of the parent or legal guardian (as may be applicable), in the manner as may be prescribed by the rules to the DPDPA.

1. Although the DPDPA prohibits the processing of personal data to undertake behavioural monitoring of children or advertisements targeting children, such a similar prohibition is not present for processing of adults' personal data. The DPDPA should recognise the principles of *Responsible AI* and allow adult data principals to either object or restrict the processing of personal data for automated decision making, profiling or targeted advertising. This right is provided under the GDPR, where the processing is undertaken by relying on the legitimate interest or if the processing is necessary for the performance of a task carried out in the public interest.
2. The Central Government can notify classes of data fiduciaries who may not be required to obtain verifiable consent or who can undertake behavioural monitoring or target advertising on children.

Research and innovation

The DPDPA provides specific exemptions to support innovation and research while balancing privacy rights. These include:

1. **Startup exemptions**: Startups notified by the Central Government are exempt from certain provisions to foster innovation and reduce compliance burdens during their growth phase, including in areas like AI and emerging technologies.
2. **Research**: Personal data may be processed for research, archiving, or statistical purposes if it is not used to make decisions specific to a data principal, and such processing is carried out in accordance with the prescribed standards to be set by the rules to the DPDPA.

Infotech Practice (Privacy and Data Protection)

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Akshaya Suresh
Partner

Drishya A. Kamath
Associate

18 Practices and
25 Ranked Lawyers

7 Ranked Practices,
16 Ranked Lawyers

Elite – Band 1 -
Corporate/ M&A Practice

---

3 Band 1 Practices

---

4 Band 1 Lawyers,1 Eminent Practitioner

12 Practices and
50 Ranked Lawyers

14 Practices and
38 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

Ranked Among Top 5 Law Firms in India for ESG Practice

Recognised in World's 100 best competition practices of 2024

Among Top 7 Best Overall Law Firms in India and
11 Ranked Practices

---

11 winning Deals in
IBLJ Deals of the Year

---

12 A List Lawyers in
IBLJ Top 100 Lawyer List

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm
of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services
Law Firm of the Year 2022

Ranked #1
The Vahura Best Law Firms to Work Report, 2022

Top 10 Best Law Firms for Women in 2022

7 Practices and
3 Ranked Lawyers

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi