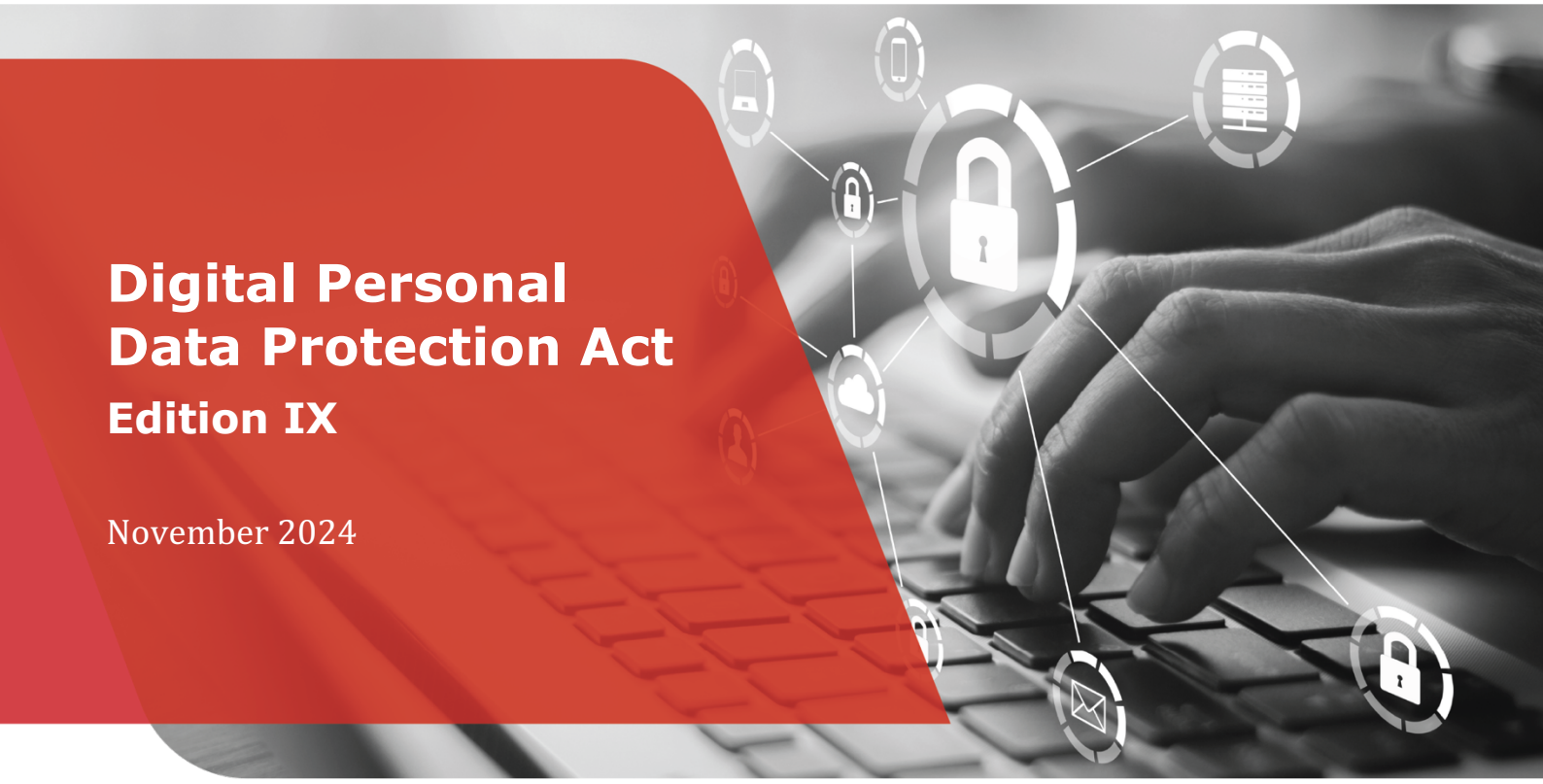
JSA Prism

Privacy and Data Protection



Digital Personal Data Protection Act

Edition IX

November 2024

Processing of employees' personal data

In this edition of the Prism, we analyse what employers would need to keep in mind while processing the personal data of their workforce. Any information about an individual collected or used even in the course of their employment is personal data under the Digital Personal Data Protection Act, 2023 ("**DPDPA**"). We also discuss the legal basis for processing an employee's personal data, an employer's key obligations, the exemptions provided in some circumstances and the challenges that employers may face in certain kinds of processing.

Transition from the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 to the DPDPA

The transition to the DPDPA marks a significant shift from the previous Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("**SPDI Rules**"), bringing a more rigorous data protection framework that requires employers to update their data management practices. Employers will need to revise internal data protection policies to align with the DPDPA, especially in areas such as employee rights and data breach management. As the SPDI Rules phase out, employers should also prepare for mandatory reporting of data breaches and ensure that internal response protocols are aligned with the DPDPA's requirements.

Roles under the DPDPA

Employer: The employer will be considered as a '*data fiduciary*'.

Employee: The employee will be considered as a '*data principal*'.

Third Parties: The third parties processing data on behalf of the employers, will be a '*data processor*'.

For example: human resources, management software

Legal basis for processing the personal data of employees under the DPDPA

The DPDPA provides certain legitimate uses under which the processing of personal data can be undertaken, without consent. One of the legitimate uses is processing personal data for the purposes of employment.

The data fiduciary can process the personal data of a data principal for:

'the purposes of employment'

or *'those related to safeguarding the employer from loss or liability such as corporate espionage'*,

'for maintenance of confidentiality of trade secrets, intellectual property, classified information'

or *'for provision of any service or benefit sought by a data principal who is an employee'*

1. It remains to be seen if, in line with international laws, the scope of 'purposes for employment' under the DPDPA include processing of personal data both before and after employment. This interpretation would encompass activities such as background verification prior to employment, as well as retaining employment records post-tenure for compliance with applicable laws.
2. The processing of personal data for service or benefit sought by a data principal may include employee training programs, employee stock option plans, medical facilities, etc.

Legal basis for processing personal data of data principals who are not considered to be 'employees'

The DPDPA does not define 'employees', creating uncertainty about the applicability of the law to other individuals working for an organisation, such as independent contractors, freelancers, consultants, temporary/part-time workers, interns, and apprentices. In the absence of a clear definition, some parallels can be drawn to interpretations in other data protection laws, where the concept of 'employment' is often understood to extend beyond traditional employment relationships. For example, some global laws treat individuals working under contractual arrangements, such as freelancers and consultants, similarly to employees when processing personal data for work-related purposes. This broad interpretation of 'employment' could influence the scope of data processing obligations under the DPDPA, even if no direct guidance is provided in the Indian context.

Relying on 'consent' to process the personal data of the above-mentioned individuals may not be meaningful since the individuals may not be able to provide 'free', and 'unconditional' consent due to the nature of the relationship between the individual and the data fiduciary.

Key considerations for employers under the DPDPA

Employer obligations under the DPDPA

Under the DPDPA, employers must adhere to several key obligations to ensure responsible data handling and protect employee personal data. First, they are required to assess processors who may be processing employee data for the DPDPA compliance before engagement and enter into a valid written contract to formalise these arrangements. Employers must also establish an internal mechanism that allows employees to exercise their rights under the DPDPA, including a grievance system to resolve concerns effectively. Additionally, implementing appropriate technical, organisational, and reasonable security measures is essential to prevent data breaches, along with a mechanism to promptly inform employees in case of such breaches. For employers classified as 'Significant Data Fiduciaries,' additional responsibilities may apply, such as appointing a data protection officer, engaging an independent data auditor, and conducting data protection impact assessments to mitigate risks.

Data retention post-employment

The employer must erase personal data once it is reasonable to conclude that the specified purpose has been fulfilled, unless retention is required to comply with any legal obligations.

Employers in India must adhere to statutory compliance by retaining specific records and employee data for mandated periods, either in original or electronic form, as outlined in various labour laws. For example, the Employees' Provident Funds and Miscellaneous Provisions Act, 1952 does not specify a clear retention period but suggests retaining records for 7 (seven) to 10 (ten) years, while the Employees' State Insurance Act, 1948 mandates 5 (five) years.

Processing of personal data of employees with disabilities

The DPDPA requires data fiduciaries, including employers, to adopt heightened safeguards when processing the personal data of employees who are persons with disabilities. The data fiduciary's responsibilities are amplified in these cases, as information related to disabilities may inherently include sensitive personal data. Such data, if disclosed or misused, has the potential to lead to discrimination or other adverse effects for the employee. Employers are therefore advised to establish specific protocols that ensure compliance with the DPDPA's mandates on data protection while also upholding principles of equality and non-discrimination.

Processing of employee data for background verification

The DPDPA does not definitively state whether 'purposes of employment' includes data collection for recruitment, such as pre-employment background checks, where an employer-employee relationship isn't yet formalised. However, the DPDPA's broad framework could reasonably support background verification as an essential step in employment, allowing employers to filter suitable candidates and manage future workforce needs. To ensure compliance, employers should clearly document the purpose of this data processing, provide necessary notifications to candidates, and follow the DPDPA requirements, minimising compliance risks. Employers frequently rely on third-party providers for high-risk data processing tasks, such as background checks, behaviour analytics, health insurance, and financial benefits. Under the DPDPA, employers should implement a thorough due diligence process and ensure that third parties processing employee data operate under formal data processor agreements with stringent security and privacy safeguards.

Managing international employee data

The DPDPA introduces specific cross-border data transfer exemptions that can reduce compliance burdens for certain fiduciaries, including employers, when handling data of non-Indian employees. These exemptions allow eligible employers more flexibility in transferring data across borders, though they must still adhere to core accountability and data security obligations under the DPDPA. Employers invoking these cross-border exemptions need to balance operational needs with ongoing compliance, as the exemptions are context-specific and require clear substantiation of eligibility. Additionally, the DPDPA grants the Central Government authority to restrict transfer of data of Indian residents to designated countries via notifications, meaning that employers must stay vigilant to ensure alignment with both the DPDPA standards and any stricter requirements imposed by other applicable laws.

Under the DPDPA, the Central Government has the authority to impose restrictions on data transfers to certain countries, which will be specified through notifications. It is crucial to note that if any other applicable law imposes stricter restrictions on an employer regarding such transfers, those restrictions will take precedence.

Startups under the DPDPA

The DPDPA has introduced a distinct category for startups, recognising the unique position they occupy within the economy and the challenges they may face in terms of compliance. A 'startup', as per the DPDPA, is a private limited company, partnership firm, or limited liability partnership that has been incorporated within India and meets specific criteria established by the Central Government's relevant department. By categorising eligible entities as startups, the DPDPA allows certain relaxations in data processing obligations, offering a more proportionate regulatory approach. For employers in this category, these relaxations aim to mitigate compliance burdens during the early stages of business growth. Nonetheless, it remains incumbent upon startups to prioritise compliance with accountability and security safeguards, as these obligations form the core of responsible data fiduciary practices under the DPDPA.

Processing of employee data to safeguard employer's interests

The processing of personal data to safeguard the employer from loss or liability is allowed under the DPDPA. The DPDPA provides a wide definition for 'loss', therefore instances such as processing of personal data for prevention of financial fraud or corporate espionage, or misuse of resources, prevention of reputational damage, or processing personal data for enforcement of legal claims, could be some of the examples for processing for safeguarding from loss or liability.

The processing of personal data to protect the employer's trade secrets, intellectual property and classified information is allowed under the DPDPA. Some of the instances for maintenance of confidentiality could include implementing access control mechanisms, to enter into non-disclosure agreements with the employees, tracking of company's information technology assets with the employees, etc.

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
42 Ranked Partners
IFLR1000 APAC Rankings 2023

Banking & Finance Team of the Year

Fintech Team of the Year

Restructuring & Insolvency Team of the Year

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

Energy - Law Firm of the Year (APAC)

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