

Employee Data and Digital Personal Data Protection Act, 2023 (“DPDP Act”)

LAW  **KNIT**

When it will be applicable?


The DPDP Act has received the Presidential assent and it will become applicable upon notification in official gazette by the Central Government. Different portions of DPDP Act may be enforced at different points of time. The penalties imposed go upto INR 250 crore (Approx USD 30 million). However, ensuring that the data fiduciary follows all requirements of the law and has taken reasonable measures to protect the data may move the Data Protection Board (DPB) to impose lesser penalties. Further, in the event of a breach, if the data fiduciary takes steps that curb such breach and prevents future breaches, the DPB may even waive penalties. This may require overhauling of the current infrastructure within the organization in a manner where you are able to track the flow of Personal Information (PI) at all times.

WHAT ARE THE IMMEDIATE PLANS & ACTIONS?

The enactment for DPDP Act requires following immediate actions on part of data fiduciaries:

- Internal due diligence of data collection and data flow
- Evaluate the portions where direct consent from Data Principal is received
- Reviewing all privacy notices
- Review whether all data collected are required for purpose
- Formulate a plan to collect updated consent
- Re-design systems - Privacy First Model/ Privacy by Design Model
- Selection & training of Grievance Officers
- Mechanism for revocation of consent

General Impact



The DPDP Act does not have a retrospective application but in cases of data collected in the past, consent may need to be procured again if the consent is not in line with the consent requirements of the DPDP Act.

Critical Issues

All persons (individual and entities) processing PI (other than for personal/domestic purpose) in India or PI of persons located in India have to abide by the requirements of DPDP Act as follows:

1. Only applicable to digitized data and for automated processing
2. Public data - made available by individual / per obligation under law, is exempted from the ambit of DPDP Act. However, there is no clarity as to the impact when a person deletes such information from public sites.
3. Data Fiduciaries are persons determining the purpose. Data processors are any person who processes on behalf of a Data Fiduciary. Only Data Fiduciaries have liability under the DPDP Act.
4. Data Principals (who shares PI) have the rights such as to: (a) access to their PI; (b) erasure or rectification; (c) grievance redressal mechanism; (d) revoke consent
5. Data Principal has the right to nominate a person - in case of death or incapacity. This means that even a deceased person's data is PI. However no period is mentioned for such requirement
6. PI can be used only for legitimate purposes and for consented purposes. Such consent has to be free, specific, informed, unconditional and unambiguous. The language of notice should be clear and simple.
7. Security measures have to be created to secure the PI.
8. Children's data, if collected have more stringent requirements - parental consent to be sought

Stages of Employment

Receipt of CV: Employer receives CV of a potential candidate which contains PI such name, contact details, salary details, financial information etc. The source could be online portals, staffing companies, internal.

Interview: This will be processed by many teams within the organisation for interview. Under deputation, client may be part of the interview and hence will be considered as transfer of information.

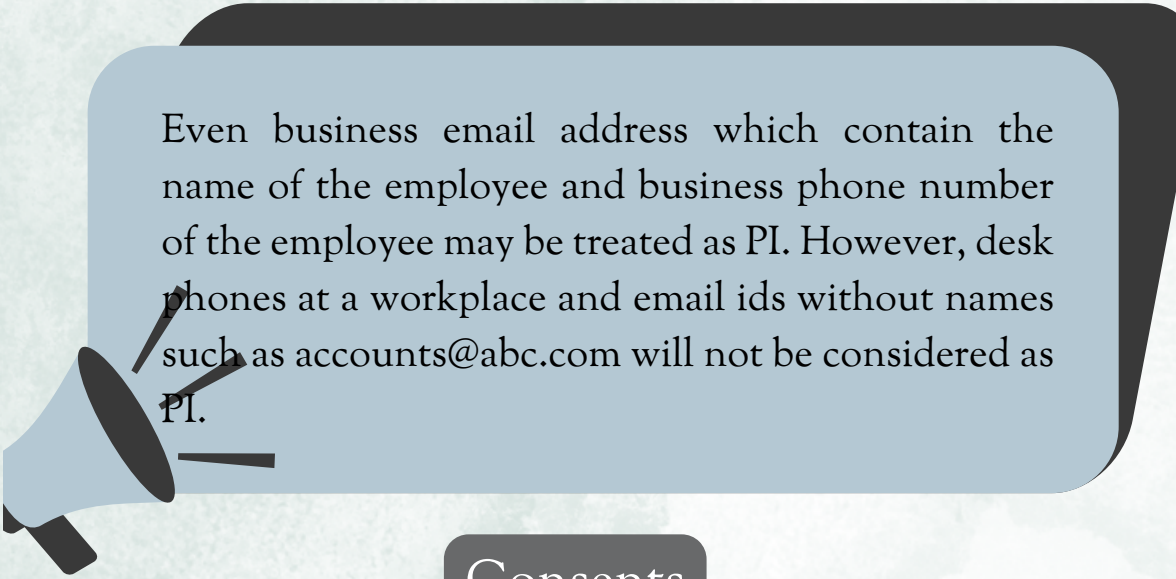
Employment: If individual is employed, then information will be used for payrolling, taxation, insurance requirements, communication, legal compliances, security requirements. These could also be outsourced.

Background Verification: Information of employees will be shared to BGV entities for processing. They may even use publicly available data for conducting BGV of the employee.

Other purposes: The information of employees could be collected for specific purposes (other than for employment) like employee survey, non essential communications, using photos for marketing purposes.

Exit: Once the employee exits the information may still be retained by the employer for statutory purposes, for creating an HR database, for ensuring compliance with non-compete or confidentiality obligations.

Employers




Even business email address which contain the name of the employee and business phone number of the employee may be treated as PI. However, desk phones at a workplace and email ids without names such as accounts@abc.com will not be considered as PI.

Consents

The DPDP Act provides that consent is not required for information that is collected for employment and for safeguarding the employer from loss or liability due to corporate espionage, confidentiality of trade secrets, intellectual property, classified information or any service or benefit sought by an employee. However, we recommend that the employer take consent from the employee/ potential employee at every stage provided above and specific consent for all types of processing done using employee PI, in the following manner:

1. General consent is to be procured prior to start of hiring process - if CV is received from an external source ensure that that person has relevant consent.
2. Add clauses in the employment contract relating to PI processing and purposes for which it is collected and manner of usage.
3. Specific consent for employee surveys, marketing/ non-essential communications, and also when processing sensitive PI .
4. Fresh consent to be sought from existing employees which should be in line with the DPDP Act.
5. Photography and image consent - for marketing specific consent to be sought.
6. Consent to be sought from ex-employees for marketing and if the employer is still using their image.

Staffing Companies



Staffing companies typically retain employee information forever. However, the DPDP Act allows you to retain information only till it serves business purpose. Hence, CVs, BGV report and other payroll information of employee will need to be deleted on a periodic basis.

Critical Issues

Staffing companies are engaged in providing human resource to their customer either on a permanent staffing model or through a temporary staffing model. In either case a lot of employee data gets processed by such entities. In this regard staffing companies need to be careful with respect to the following:

1. Ensure that consent is collected from the candidate for all information collected and even for processing by the client.
2. Ensure that data processing agreements are entered into with client wherein you have a joint fiduciary relationship with the client and not that of a fiduciary- processor relationship. Under joint fiduciary relationships both parties will be (a) defining the purpose for collection; and (b) jointly responsible for any breaches or lapses in compliance. The agreement should clearly define the responsibilities, liabilities and indemnities of each party.
3. Check the data retention period with respect to CVs that are received and BGV reports generated - this should align with regulatory requirements.
4. Drug tests, if carried out, might fall under more sensitive category of information and might make you a significant data fiduciary (SDF). Being an SDF shall attract more compliances such as conducting a data privacy impact assessment, appointment of a data protection officer who is based in India, conducting periodic audits etc.
5. If large amounts of data of employees are collected by the entity, the staffing agency may be categorised as an SDF.

How can we help?

We can assist the Client and their HR team with the following:

- Conducting Gap Analysis with the current format of the organization
- Advisory and assisting in implementation by organizations
- Providing documentation assistance in relation to Data Processor and Data Fiduciary agreements, consent mechanisms

Disclaimer: This document has been made for generic information and discussion perspective and shall not be considered as legal advice. No one should act or advise to act on it without seeking proper legal advice.

KNIT-KNOW-AI

LAWKNIT KNOWLEDGE ASSISTANT

Disclaimer: This knowledge product leverages machine learning, algorithmic intelligence and language model/s for prompts based legal information and awareness; however, it channelizes to data dependent and AI generated responses that should neither be construed as comprehensive and latest, nor be considered as a legal advice in part or full, and they should always be verified for accuracy, completeness, reliability, quality and validity. Besides, we shall not be liable at any stage for any inadvertent info biases, content errors and timeline gaps, and shall not be under any compulsion for any data maturity versions and model training iterations.

We are here to help you understand the scope of data protection laws and answer any questions you may have regarding the processing of personal data.

You can ask me any questions. e.g:

1. What are the rights of a data principal under the data protection laws?
2. How can I make a complaint to the Data Protection Board?
3. What are the obligations of a

Type your message...



AA

lawknit.co



The Digital Personal Data Protection Bill, 2023 was passed in Parliament and received presidential assent on August 12, 2023. The Digital Personal Data Protection Act, 2023 (“DPDP Act”) is applicable to the processing of all kinds of digital personal data within India irrespective of data being collected online or offline. It is also applicable to the processing of personal data outside India if it is for offering goods or services in India. The Act also grants certain rights to individuals which includes the right to seek correction and erasure, obtain information and grievance redressal mechanism. Some of the details of DPDP Act is as follows for further feel free to access our DPDP AI- KNIT KNOW-DP



For Queries reach out to us:
Clients: Create query on LawKNIT platform

Non-Clients: write to us
arunabh@lawknit.co

