HANDLING RESUME SUBMISSIONS UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT

1. INTRODUCTION

The Digital Personal Data Protection Act, 2023 **(the "DPDP Act"),** which introduces comprehensive obligations for handling personal data[1], grants the employers significant flexibility through the legitimate use exemption, allowing them to process employment-related personal data (names, addresses, contact information, financial record, biometric information etc.) without explicit consent when necessary for employment purposes including recruitment processes. This article explores the implications of the DPDP Act on resume handling and provides guidance for employers to ensure compliance while respecting the candidate's privacy and maintaining efficient recruitment practices.

The DPDP Act establishes a clear hierarchy of roles in the data processing ecosystem. When a candidate submits their resume to an organization, they become a "Data Principal[2]"- the individual to whom the personal data relates. The organization receiving and processing this information assumes the role of a "Data Fiduciary[3]," as they determine how and why the candidate's personal data will be processed. In cases where organizations engage external services such as recruitment agencies or background verification companies, these third parties are designated as "Data Processors[4]," processing personal data on behalf of the Data Fiduciary.

2. CONSENT MANAGEMENT REQUIREMENTS

The DPDP Act introduces nuanced requirements for consent management that vary depending on how resumes are submitted. Based on the industry practice, we contemplate the following two scenarios:

Scenario 1: When the candidate directly submits their application through email or in person

When a candidate directly submits their application to the organization through email or in person, the DPDP Act considers this a voluntary sharing of information that falls under the legitimate use exemption. The DPDP Act's "legitimate use"[5] provision lets the employer to collect and use employee data without seeking explicit consent when needed for the purpose of employment or to protect the company interests. This includes preventing corporate espionage, safeguarding trade secrets, maintaining confidentiality, and providing employee benefits. Simply put, companies can legally process employee information without permission when it directly relates to the job or helps protect the business from potential losses. The candidate in this scenario is considered to be providing implicit

---

[1] Section 2(t) Digital Personal Data Protection Act, 2023 defines "Personal Data" as any data about an individual who is identifiable by or in relation to such data.
[2] Section 2(j) Digital Personal Data Protection Act, 2023 defines "Data Principal" as any individual to whom the personal data relates and where such individual is (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.
[3] Section 2(i) of the Digital Personal Data Protection Act, 2023 defines "Data Fiduciary" as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
[4] Section 2(k) of the Digital Personal Data Protection Act, 2023 defines "Data Processor" as any person who processes personal data on behalf of a Data Fiduciary.
[5] Section 7 of the Digital Personal Data Protection Act, 2023, says that A Data Fiduciary may process personal data of a Data Principal for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

consent for the organization to process and store their personal data, for employment or internship purposes. This voluntary submission is generally interpreted as permission for the organization to use the information not only for the immediate hiring process but also for future employment opportunities within the organization.

Scenario 2: When the candidate is required to provide data to an online portal

When a candidate enters their personal information through the organization's online recruitment portal, the requirements change significantly. In these cases, organizations must implement more stringent consent management protocols. The portal must explicitly request and obtain the candidate's consent before processing their personal data. Organizations are required to provide clear, and detailed information about how the data will be used, including specific information about data retention policies. They must also explicitly state whether the information will be retained for future opportunities and obtain separate consent for this purpose.

3. DATA RETENTION AND DELETION PROTOCOLS

Notwithstanding the scenarios described above, the DPDP Act mandates strict protocols for data retention and deletion that organizations must follow diligently when a candidate is not selected for a position. The organization is required to delete all personal information collected during the recruitment process, unless there is a specific legal requirement for retention. Even in cases where legal mandates require data retention, organizations must obtain explicit consent from candidates before continuing to store their personal data. This process must include clear communication about the purposes of retention and its duration. Organizations must also ensure that candidates are fully informed of their right to withdraw consent at any time.

4. ORGANISATIONAL RESPONSIBILITY AND RECOMMENDED BEST PRACTICES

Further, as data fiduciaries under the DPDP Act, organizations bear significant responsibilities in protecting candidate data. Organizations must ensure compliance with the DPDP Act's requirements, whether they process data internally or through third-party data processors. This includes maintaining the accuracy and completeness of personal data, implementing appropriate technical and organizational security measures, and processing data only for specified purposes and durations. Organizations must establish robust mechanisms that allow candidates to access information about their personal data and request its erasure when appropriate. A well-structured grievance redressal system must be in place, complete with publicly available response timeframes that give data principals clear expectations about when their concerns will be addressed. In the event of a personal data breach, organizations must notify the affected candidates through registered communication channels with all information prescribed under the DPDP Act.

To ensure comprehensive compliance with the DPDP Act, we recommend that organizations should implement the robust framework of best practices. This begins with developing clear, and detailed policies for handling application data and providing regular training to HR personnel on data protection requirements. Organizations must implement secure systems for storing and processing applications, establishing clear procedures for handling candidate data requests. It's essential to maintain comprehensive documentation of all data processing activities and regularly review and update security measures to address evolving threats and requirements.

5. CONCLUSION

The DPDP Act represents a significant evolution in how organizations must handle resume submissions and candidate data in India. By thoroughly understanding the distinctions between different submission methods and implementing appropriate protective measures, organizations can maintain compliance while effectively managing their recruitment processes. Success in this area requires ongoing commitment to reviewing and updating practices to ensure continued alignment with the DPDP Act's requirements and the protection of candidate data. Organizations that invest in robust data protection measures not only ensure legal compliance but also build trust with candidates and protect their reputation in the recruitment marketplace.

Authors: Debjani Aich, Varsha D. Sinchana, Riddhi Jain.

Date: February 19, 2025

Practice Areas: **Labour and Employment Law**

DISCLAIMER