GUIDANCE NOTE

India - Employment

Abe Abraham
CYRIL AMARCHAND MANGALDAS



Luv Saggi
CYRIL AMARCHAND MANGALDAS



Abhilash Tyagi
CYRIL AMARCHAND MANGALDAS



6 days ago

March 2025

1. Laws

1.1. Laws and regulations

1.1.1. What laws and/or regulations apply to data protection in the employment context?

Currently, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2021, enacted under the Information Technology Act, 2000 (the IT Act), is the primary legislation in India that governs data protection in the employment context.

However, the Government of India is in the process of implementing the Digital Personal Data Protection Act, 2023 (the Act), which once implemented, will be the primary legislation governing data protection in the

employment context. The Act received the President of India's assent on August 11, 2023, but its effective date is yet to be notified in the Official Gazette. The Draft Digital Personal Data Protection Rules, 2025 (the Draft Rules) framed under the Act, have been released for public consultation. Following this consultation, the finalized rules will be consolidated and notified, fully operationalizing the new framework of the data protection law in India. The Act applies to the processing of digital personal data within India when the data is either collected in digital form or initially in non-digital form but later digitized. Additionally, it extends to the processing of digital personal data outside India if it pertains to activities such as offering goods or services to Data Principals located within Indian territory.

The term 'personal data' refers to any information that can identify an individual, either directly or indirectly. 'Processing' includes a broad range of activities such as collection, storage, use, transfer, or even erasure of such personal data.

Having said that, provisions of the Act do not apply to personal data collected/processed by an individual for any personal or domestic purpose (such as maintaining a contact list on the phone for personal use). Additionally, the Act does not apply to the personal data which relates to the data principle made publicly available by the data principle, or if the personal data that relates to the data principle was made public by any other person who was under an obligation under the law to make that personal data publicly available (such as judges obligations to publish judgments/orders to make it public).

Citation	Not applicable.

1.2. Supervisory authority

1.2.1. Who is responsible for enforcing the law(s) and issuing guidelines?

The Data Protection Board of India (the Board) is the supervisory authority responsible for enforcing the provisions of the Act. The Board is tasked with ensuring compliance with the provisions of the Act, handling grievances, and imposing penalties for non-compliance therein. It serves as the primary public forum for addressing disputes between data principals (herein employees or candidates) and data fiduciaries (entities processing data or employers). That

said, before approaching the Board, employees (data principals) must exhaust their opportunity to redress their grievances under the grievance redressal mechanism established by the data fiduciary (employer) (Section 13 of the Act).
In addition to its adjudicatory functions, the Board plays an important role in monitoring data breaches. Under the Act, Data Fiduciaries are required to notify the Board and affected individuals in the event of a data breach (Section 8(6)). The Board is empowered to investigate such breaches, recommend remedial measures, and impose penalties (Section 27 of the Act).

Beyond the Board, the Central Government exercises significant authority under the Act. For example, it has the power to:

- restrict, via notifications, cross-border data transfer of personal data by employer/data fiduciary for processing (Section 16 of the Act); and
- notifying exemptions for certain classes of data fiduciaries (e.g., startups) easing compliance requirements for smaller organizations (Sections 17(3) and 17(5) of the Act).

Together, the Board and the Central Government form a dual-layered framework for enforcing data protection and providing guidance.

Citation	Sections 8(6), 13, 16, 17(3), 17(5), 18, and 27 of the Act

1.3. Guidelines

1.3.1. Have any guidelines been released on data protection in the employment context?

The Draft Rules are the only legislative framework expected to provide detailed operational guidance under the Act.

Further, as discussed in our response above, once the Act and the Draft Rules are implemented, the Central Government has the power to issue notifications on various aspects governed by the Act and the Draft Rules.

Citation	Not applicable.

2. Recruitment and selection

2.1. Hiring documents

2.1.1. Is it permissible to collect hiring documents?

Yes, it is permissible to collect hiring documents. However, to the extent such hiring documents fall within the ambit of 'personal data' (i.e., any data about an individual who is identifiable by or in relation to such data), it can only be processed (which also includes the collection of personal data):

- with the consent of the data principal (candidate or employee); or
- for 'certain legitimate uses' as prescribed under the Act.

It is hereby clarified that if the personal data intended to be processed falls within the scope of 'certain legitimate uses' as defined under Section 7 of the Act, there is no requirement to obtain consent of the data principal.

Citation	Sections 4 and 7 of the Act

2.1.2. Are there any restrictions on collecting hiring documents?

Yes, there are specific restrictions on the collection of hiring documents under the Act (to the extent such hiring documents fall within the ambit of personal data). Employers must comply with the following limitations.

- Data minimization

Employers are restricted from collecting more personal data than necessary for the recruitment process. As per Sections 4(1) and 6(1) of the Act, the data collected must be limited to what is directly relevant and necessary for the specified purpose (e.g., evaluating the candidate's qualifications or work authorization). For instance, collecting financial data unrelated to the role would violate this principle.

- Purpose limitation

Any personal data, including hiring documents, can only be collected and processed for a defined, lawful purpose. When consent is the legal basis for collecting personal data, employers cannot process data for any purpose beyond what has been communicated in the notice to the candidate (Section 4(1) of the Act). For example, if the notice specifies that data will be used only for recruitment, it cannot later be used for marketing purposes without additional consent. Additionally, regardless of what purpose has been provided in the notice for collecting/processing such personal data, the personal data collected should actually be necessary for the purpose specified in the notice (Section 6(1) of the Act).

Where personal data falls within the scope of 'certain legitimate uses' as defined under Section 7 of the Act, where consent is not required, and no notice is mandated, the same principles mentioned above must be followed. The personal data processed must fall squarely within the defined scope of legitimate purposes, and the processing must be strictly necessary for those purposes. While the provisions of the Act are not explicit about these, they align with the general principles of the Act, which emphasize purpose limitation and necessity in processing personal data.

- Consent invalidity for unlawful requests

Any request for consent that infringes the Act or other applicable laws will be invalid to the extent of such infringement (Section 6(2) of the Act). For example, requesting consent to waive the candidate's right to file a grievance would be considered unlawful and unenforceable.

Additional obligations/restrictions on the handling of personal data, including hiring documents

In addition to the obligations/restrictions outlined above, the Act and accompanying the Draft Rules impose additional obligations/restrictions on data fiduciaries regarding the management of personal data including hiring documents, after it has been collected. These include obligations related to retention, erasure, and withdrawal of consent, and the responsibility to ensure that personal data is updated and accurate. These obligations primarily arise under Sections 6 and 8 of the Act, alongside Rule 8 of the Draft Rules. To understand the additional restrictions on handling personal data, we have broken down the key obligations and provided our interpretation of them in the sections below.

- Retention, erasure, and withdrawal of consent

Under the Act's framework, employers cannot retain personal data, including hiring documents, indefinitely, where consent is the legal basis for processing/collecting such personal data. Obligations to erase and cease processing personal data arise under Sections 8(7) and 8(8) of the Act and the provisions governing consent withdrawal under Section 6 of the Act. These provisions ensure that personal data is managed responsibly and is not retained or processed beyond its intended purpose.

- Withdrawal of consent

Under Section 6(4) of the Act, the data principal has the right to withdraw consent at any time. When this occurs, the data fiduciary must cease processing and erase the personal data within a reasonable time (Section 6(6) of the Act) and ensure that any data processor acting on its behalf also ceases processing and erases the personal data of the data fiduciary.

- Retention linked to the specified purpose

As per Section 8(7) of the Act, personal data must be erased once it is reasonable to assume that it is no longer required for the specified purpose unless retention is mandated by law. The specified purpose is tied to the notice provided to the data principal under Section 5 of the Act mentioning the purpose for processing the personal data.

Please note that for a data fiduciary belonging to a specified class and processing personal data or related purposes as outlined in the Third Schedule, Section 8 of the Act, along with Rule 8 of the Draft Rules, establishes guidelines (including the specified time period) for determining when a purpose is considered to be no longer served. For instance, the Third Schedule has specific guidelines for determining when the purpose is considered to be no longer served for data fiduciaries who is an online gaming intermediaries have not less than 50,00,000 registered users in India.

Can an employee's right to withdraw consent, cessation of processing, and erasure of personal data under Sections 6 and 8 be enforced for certain legitimate uses including for the purposes of employment?

Illustrations under Section 7(a) of the Act indicate that when employees (data principals) voluntarily provide their personal data, they retain the right to

withdraw consent, cease processing, and have the data erased. For example, if an employee shares their resume for hiring purposes, they should be able to withdraw it, requiring the employer to cease processing and erase the data. However, other portions of Section 7 of the Act present a distinct scenario. Under this provision, certain legitimate uses of personal data, including employment-related processing, are exempt from consent and notice requirements. Since Section 7 of the Act does not explicitly require consent or notice, data processed under this section is not strictly tied to a 'specified purpose' in the way data collected under consent-based frameworks would be. As a result, provisions of Section 6 (withdrawal of consent and cessation of processing) and Section 8 (erasure) do not automatically apply to such data, as we have discussed in earlier responses. However, this does not mean that the concept of purpose limitation should be narrowly interpreted. While Section 7 of the Act does not impose the same level of restriction as consent-based processing, it does not suggest that data may be processed indefinitely without any connection to a valid purpose. A reasonable interpretation would be that even where data is processed under a legitimate purpose, it should still be subject to the broader principles of necessity and purpose limitation to ensure that processing remains justified.

Technically, Section 7 of the Act should be interpreted to mean that data must only be processed as long as it continues to serve its intended purpose. This means that once the data no longer fulfills that purpose, it should fall outside the scope of Section 7 (including for purposes of employment), and its retention or further processing should not be justified. For example, if an employer collects an applicant's data to verify work eligibility, that data remains relevant only for the duration of employment. Once employment ends, the legal basis for retaining such data ceases, and it should no longer be processed or retained indefinitely.

Accuracy and rights to correction

Another significant obligation under the Act is ensuring that personal data, including hiring documents, is accurate, complete, and up to date. Section 8(3) of the Act makes it clear that employers must take reasonable steps to ensure that personal data remains accurate and up to date.

Citation	Sections 4, 5, 6, 7 and 8 of the Act

2.1.3. Which lawful bases can be relied on for the processing of personal information contained in hiring documents?

As per Section 4 of the Act, there are only two legal bases that can be relied on for processing personal data, including hiring documents which are as follows:

- with the consent of the data principal (e.g., candidate or employees); or
- for 'certain legitimate uses' as provided under Section 7 of the Act.

While consent-based processing is straightforward, the scope of certain legitimate uses under Section 7 of the Act is broader but requires careful interpretation to avoid overreach or non-compliance. Below, we examine these lawful bases:

Consent requirement

Where consent is the legal basis for processing personal data, the Act requires that consent must be free, specific, informed, and unambiguous with a clear affirmative action (Section 6(1) of the Act). These terms, while not explicitly defined in the Act, can be interpreted to mean the following:

- Free

This can be interpreted to mean that consent must be obtained without any form of compulsion, pressure, or implicit threat that forces the data principal (candidate) to agree. For example, if a candidate is informed that their refusal to provide consent for processing personal data unrelated to the hiring process would result in the rejection of their application, such consent would not qualify as free. The individual must have the freedom to decline consent without fear of negative consequences, and their choice should not be influenced by deceptive or coercive practices. 'Free' implies a clear and voluntary decision, untainted by pressure or manipulation.

- Specific

This can be interpreted to mean that consent must be sought for a clearly defined and particular purpose. For instance, if the employer collects a candidate's data for recruitment purposes, the employer must specify the precise activities involved, such as verifying qualifications or conducting

background checks. General or blanket consent that covers undefined or broad purposes, such as 'future business requirements,' would not meet this criterion. The specific nature of consent ensures that the candidate knows exactly what they are agreeing to.

- Informed

This can be interpreted to mean that the data principal (candidate) must be provided with all relevant information to make an informed decision before giving consent. Adding to this Section 5 of the Act also requires that every consent request must be accompanied or preceded by a notice given by the data fiduciary to the data principal informing the latter about various aspects of the personal data collected including the purpose and rights the data fiduciary can exercise in relation to their personal data collected.

- Unambiguous with a clear affirmative action

This can be interpreted to mean that the candidate's consent must be expressed explicitly and unmistakably. For example, a candidate ticking a box or clicking 'I agree' to a specific consent statement on an application portal qualifies as a clear affirmative action. Silence, pre-ticked checkboxes, or implied consent through inactivity would not satisfy this requirement. The clarity of affirmative action ensures that there is no ambiguity about the candidate's agreement.

The above interpretations are based on a broader understanding of the text of Section 6(1) of the Act. As the Act has not yet been enforced, and no case law or authoritative guidance currently exists on the interpretation of these terms, the meanings provided here are our reasoned understanding and may evolve based on future enforcement decisions or judicial precedents.

Additionally, it is important to note that the Act specifies that every request for consent must be presented to the data principal in a clear and plain language, giving them the option to access such request in English or any language specified in the Eighth Schedule to the Constitution of India (the Constitution) and providing the contact details of a data protection officer (DPO), where applicable, or of any other person authorized by the data fiduciary to respond to any communication from the data principal for the purpose of exercising of her rights under the provisions of this Act.

Certain legitimate uses

Section 7 of the Act provides scenarios where personal data may be processed without the need to obtain consent. These provisions are relevant to employment contexts but come with ambiguities regarding their application to hiring documents and pre-employment processes. The following subsections address the key provisions which are relevant in the employment context:

Voluntary provision of personal data

Where a data principal voluntarily provides personal data for a specific purpose, the employer may process this data unless the individual objects. For instance, when a candidate submits their CV or cover letter, this could be interpreted as a voluntary provision of personal data for recruitment purposes. However, processing must be limited to the specified purpose. For example, if a candidate submits data for a job application, it cannot be repurposed for unrelated activities like marketing without additional consent.

Purposes of employment and related uses

This provision allows the processing of personal data for:

- the purposes of employment; or
- safeguarding the employer from loss or liability, such as:
- preventing corporate espionage;
- maintaining confidentiality of trade secrets, intellectual property, and classified information; and
- provision of services or benefits sought by the Data Principal (employee).

While this clause provides a broad basis for processing, its scope has been narrowed compared to earlier drafts of the legislation. A key change in the final Act is the shift in language from 'related to employment' in the 2022 version of the Data Protection Bill to 'of employment,' restricting the scope of permissible processing of personal data. The earlier draft not only used the broader phrase 'related to employment' but also explicitly included terms such as 'recruitment,' 'verification of attendance,' and 'assessment of performance,' making it clear that these activities were meant to be covered. However, in the Act, these terms have been omitted, and the phrase 'of employment' has replaced 'related to employment,' indicating a narrower intent. While legislative omissions can sometimes be a matter of drafting efficiency, the

combined effect of these deletions and the shift in phrasing suggests a deliberate move to limit the provision's scope to data processing strictly related to core employment activities, rather than extending to ancillary HR functions.
Similarly, it does not explicitly extend to non-employee engagements, such as consultants, freelancers, or gig workers. In such cases, reliance on consent or other provisions may be required.

Legal and statutory obligations

Employers may process personal data without consent to fulfill legal or statutory requirements. Based on our understanding of the Act, some of the examples that are most likely to be covered under Section 7(d) of the Act are:

- verifying work authorization to comply with labor laws;
- using personal data for payroll reporting and tax compliance; and
- maintaining hiring records to demonstrate adherence to workplace safety and anti-discrimination laws.

Please note that processing must remain strictly limited to the legal obligation being fulfilled, and unrelated data must not be processed.

In light of the above, we believe that hiring documents, which contain personal data essential to core employment activities, should ideally fall within the scope of Section 7(i) of the Act, as they are intrinsically linked to employment itself. Additionally, any personal data within these documents that must be processed to comply with legal requirements should be covered under Section 7(d) of the Act, ensuring that consent is not required in both cases.

Recommendations

The narrowing of Section 7(i) of the Act reflects an effort to limit the scope of processing without consent, particularly in pre-employment contexts. However, the lack of explicit guidance in the Act and Draft Rules leaves significant room for interpretation. Therefore, from the best practices perspective and to mitigate any potential legal risks, we recommend the following practices should be adopted by the employers.

- For ambiguous activities, such as background verification or psychometric tests, obtaining explicit consent is advisable to mitigate

risks.

- Employers must carefully assess whether such activities are truly necessary for the employment relationship or require explicit consent.
- Employers should maintain records demonstrating that processing under Section 7 of the Act is both necessary and proportional to the specified purpose.

Employers should obtain consent for processing data related to consultants, freelancers, or gig workers, as Section 7(i) of the Act does not explicitly cover such roles.

Citation	Sections 4, 5, 6, and 7 of the Act

2.1.4. Is it permissible to disclose/share such personal information with third parties?

The disclosure of personal information under the Act is expressly considered a form of processing as defined under the Act. Section 2(x) of the Act defines processing broadly to include operations such as collection, storage, use, sharing, dissemination, and disclosure of personal data. Therefore, disclosure is inherently covered under the ambit of processing, and all the principles and safeguards applicable to data processing also extend to disclosures. This means that when disclosing digital personal data, the same obligations of lawfulness, purpose limitation, data minimization, and security measures apply.

Any disclosure must align with a lawful basis, either through the consent of the data principal or under the certain legitimate uses outlined in Section 7 of the Act. For instance, hiring documents such as CVs, references, or interview notes may be disclosed to state authorities for compliance purposes under Section 7(c) of the Act or shared with an arbitration court for resolving disputes under Section 7(e) of the Act.

The Act also allows for personal data to be shared with a data processor provided such sharing is conducted under a valid contractual arrangement as required by Section 8 of the Act. Also, Section 8(3)(b) of the Act specifically mandates if the personal data is likely disclosed to another data fiduciary, such personal data should be complete, accurate, and consistent. The data processor is obligated to process the data strictly in accordance with the data fiduciary's instructions and only for the specified purpose. For example, if an

external agency is engaged to conduct background checks as part of the hiring process, the data can only be shared under a contract ensuring it is used solely for verification purposes, with clear safeguards to prevent unauthorized sharing or misuse. The contract must also ensure that the data processor complies with all security measures to protect the personal data from breaches or unauthorized access.

Citation	Sections 2, 7, and 8 of the Act

2.1.5. Is notice required when collecting such data?

Yes, notice is required under the Act when collecting personal data from a data principal where consent is the legal basis for processing the data. Section 5 of the Act mandates that any request for consent under Section 6 of the Act must be accompanied or preceded by a notice from the data fiduciary.

While not explicitly provided, in our view, a general notice requirement should also extend to personal data processing under Section 7 of the Act, which allows processing for certain legitimate purposes, including employment-related purposes. This would inform employees about the purpose for which their personal data is being processed.

Additionally, under Section 5 of the Act, notice requirements ensure that employees/candidates (as data principals) are informed about their rights. Therefore, when processing personal data under Section 7 of the Act, including for employment purposes, it would be consistent with the broader principles of the Act for employers (as data fiduciaries) to provide a notice covering key details about data processing.

Citation	Sections 5, 6, and 7 of the Act

2.1.6. What information must be provided with the notice?

The notice must include the following minimum details as per Section 5 of the Act and Rule 3 of the Draft Rules.

- Itemized description of personal data: Clearly specify the categories of personal data being collected.

- Specified purpose of processing: Provide a clear description of why the data is being collected and how it will be used. Further, there must be an itemized description of the goods and services to be provided or uses to be enabled by such processing.
- Details of rights and complaint mechanisms should include the following.
    - How the Data Principal can exercise their rights under Section 6(4) of the Act (e.g., withdrawing consent) and Section 13 of the Act (e.g., grievance redressal).
    - The process for withdrawing consent and exercising rights.
    - How to make a complaint to the Board.
    - Link to additional information: A link to the website or app of the data fiduciary for accessing this information, along with other means, if any, to exercise their rights or file complaints.

Citation	Section 5 of the Act Rule 3 of the Draft Rules

2.1.7. In what format must this information be provided?

As per Section 5(3) of the Act and Rule 3(a) of the Draft Rules, the notice must be presented in a manner that is understandable independently of any other information, it should:

- be provided in clear and plain language;
- include an option to access the contents of the notice in English or any language specified in the Eighth Schedule to the Constitution; and
- be accessible through a communication link (e.g., a website or app) provided by the data fiduciary.

Citation	Section 5(3) of the Act Rule 3(a) of the Draft Rules

2.1.8. When should notice be provided?

The notice must be provided before or at the time of collecting data. Under Section 5(1) of the Act, the notice must accompany or precede any request

for consent from the data principal.

If personal data was collected before the Act's commencement, Section 5(2) of the Act requires that the data fiduciary, as soon as reasonably practicable, provide the data principal with a notice detailing the purpose of processing their rights under the Act, and the complaint mechanism.

Citation	Section 5 of the Act

2.2. Special category data

2.2.1. Is it permissible to collect special category data during recruitment?

Please refer to section 2.1.3. above and the corresponding questions addressed within that section in relation to background checks.

Citation	Sections 4, 5, 6, and 7 of the Act

2.2.2. Are there any restrictions on collecting special category data during recruitment?

Please refer to section 2.1.2. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, 7, and 8 of the Act

2.2.3. Which lawful bases can be relied on for the processing of special categories of data during recruitment?

Please refer to section 3.4.3. below and the corresponding questions addressed within that section.

Citation	Sections 4,5,6, and 7 of the Act

2.2.4. Is it permissible to disclose/share such personal information with third parties?

Please refer to section 2.1.4. and the corresponding questions addressed within that section.

Citation	Sections 2,7, and 8 of the Act

2.2.5. Is notice required when collecting such data?

Please refer to section 2.1.5. and the corresponding questions addressed within that section.

Citation	Sections 5,6, and 7 of the Act

2.2.6. What information must be provided within the notice?

Please refer to section 2.1.6. and the corresponding questions addressed within that section.

Citation	Section 5 of the Act Rule 3 of the Draft Rules

2.2.7. In what format must this information be provided?

Please refer to section 2.1.7. and the corresponding questions addressed within that section.

Citation	Section 5(3) of the Act Rule 3(a) of the Draft Rules

2.2.8. When should notice be provided?

Please refer to section 2.1.8. and the corresponding questions addressed within that section.

Citation	Section 5 of the Act

3. Employee records

3.1. Personnel records

3.1.1. Is it permissible to process personal information contained in personnel records?

Please refer to section 2.1.1., and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, and 7 of the Act

3.1.2. Are there any restrictions on processing such data?

Please refer to section 2.1.2. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, 7, and 8 of the Act

3.1.3. Which lawful bases can be relied on for processing personal information contained in personnel records?

Please refer to section 2.1.3. and the corresponding questions addressed within that section.

Processing personal records such as identification details, right-to-work documentation, bank details, addresses, contact information, and national identification numbers is essential for employment management. These are not ancillary HR functions but core employment activities, as they are necessary for payroll administration, taxation compliance, social security contributions, and workplace verification. Without these records, an employer cannot effectively maintain an active employment relationship.

While the shift in language from 'related to employment' in the 2022 Data Protection Bill to 'of employment' in the final Act has restricted the scope of permissible data processing, personal records should still logically fall within

this framework as they are integral to an employee's ongoing employment. Additionally, certain records, such as national identification numbers, are required for statutory obligations like provident fund contributions and taxation compliance, aligning with Section 7(d) of the Act, which allows processing for legal obligations. The broader necessity of maintaining/processing personal records for employment administration should ideally be covered under Section 7(i) of the Act as well.

Citation	Section 7 of the Act

3.1.4. Is it permissible to disclose/share such personal information with third parties?

Please refer to section 2.1.4. and the corresponding questions addressed within that section.

Citation	Sections 2,7, and 8 of the Act

3.2. Performance records

3.2.1. Is it permissible to process personal information contained in performance records?

Please refer to section 2.1.1. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, and 7 of the Act

3.2.2. Are there any restrictions on processing such data?

Please refer to section 2.1.2. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, 7, and 8 of the Act

3.2.3. Which lawful bases can be relied on for processing personal information contained in performance records?

Please refer to section 2.1.3. and the corresponding questions addressed within that section.

As explained in our previous responses, please note that there has been a shift in the language from 'related to employment' in the 2022 Data Protection Bill to 'of employment' in the final Act, thereby restricting the scope. Additionally, explicit references to performance management, which were included in the earlier 2022 Bill, have been omitted from the Act.

Having said that, we believe that performance management is a core employment activity and should ideally fall even within the restrictive ambit of 'of employment.' Managing promotions, grievances, disciplinary actions, and bonuses is integral to the employer-employee relationship and directly impacts workplace operations, employee retention, and overall workforce governance. Given this fundamental role, such data processing should be considered necessary for employment rather than an ancillary function requiring separate justification. Therefore, in our view, processing performance-related records should not necessarily require consent.

Citation	Section 7 of the Act

3.2.4. Is it permissible to disclose/share such personal information with third parties?

Please see section 2.1.4. and the corresponding questions addressed within that section.

Citation	Sections 2,7, and 8 of the Act

3.3. Activity records

3.3.1. Is it permissible to process personal information contained in activity records?

Please refer to section 2.1.1. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, and 7 of the Act

3.3.2. Are there any restrictions on processing such data?

Please refer to section 2.1.2. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, 7, and 8 of the Act

3.3.3. Which lawful bases can be relied on for processing personal information contained in activity records?

Please refer to section 2.1.3. and the corresponding questions addressed within that section.

Activity records, such as attendance, annual leave, and incident reports, play an essential role in managing employment relationships. However, whether they fall under Section 7 of the Act depends on the specific purpose and context of their use.

Attendance records

Tracking attendance is an essential part of employment management, directly impacting payroll, compliance, and workforce administration. It is not an ancillary function but a fundamental aspect of an individual's ongoing employment. While there has been a shift in language from 'related to employment' in the 2022 Bill to 'of employment' in the Act, thus narrowing the scope of permissible data processing, and despite the omission of 'verification of attendance' from the Act, attendance records should still logically be included within the scope of employment-related processing. Unlike discretionary HR functions, attendance tracking is an operational necessity tied directly to an employee's active engagement in the workplace. Therefore, even within this narrower framework, processing attendance records should ideally be covered.

Annual leave records

Many employment laws, such as state-specific Shops and Establishment Acts, require employers to maintain leave registers as part of statutory compliance. In such cases, processing annual leave records aligns with Section 7(d) of the Act, which allows data processing to fulfill legal obligations. Further, processing of employees' annual leave records is a core employment activity

and should even therefore fall under the restrictive ambit of 'purposes of employment.' However, if these records are used for any additional purposes, obtaining employee consent is advisable.

Incident Reports

Incident reporting is typically tied to legal obligations. For example, under the Employees' Compensation Act, 1923, employers are required to report accidents to the authorities. In such scenarios, processing this data falls under Section 7(d) of the Act as a legal requirement. Since these records are explicitly linked to statutory compliance, consent is not necessary.

Citation	Section 7 of the Act

3.3.4. Is it permissible to disclose/share such personal information with third parties?

Please refer to section 2.1.4. and the corresponding questions addressed within that section.

Citation	Sections 2,7, and 8 of the Act

3.4. Sensitive records

3.4.1. Is it permissible to process personal information contained in special category records?

Please refer to section 2.1.1. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, and 7 of the Act

3.4.2. Are there any restrictions on processing such data?

Please refer to section 2.1.2. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, 7, and 8 of the Act

3.4.3. Which lawful bases can be relied on for processing personal information contained in sensitive records?

Please refer to section 2.1.1. and the corresponding questions addressed within that section.

Certain categories of sensitive personal data, such as criminal data, diversity data, and medical records, may be processed as part of employment-related activities, but the extent to which they fall under employment purposes as defined in Section 7 of the Act remains unclear. As discussed earlier, the shift in language from 'purposes related to employment' (in the earlier 2022 Bill) to 'purposes of employment' suggests a more restrictive scope, possibly limited to core employment-related tasks.

However, sensitive data such as diversity data or medical records could also potentially fall under other subsections of Section 7 of the Act, such as Section 7(i), where data can be processed without consent if it is required to provide an employee benefit (e.g., health benefits). Similarly, Section 7(d) of the Act allows the processing of data without consent if required to comply with legal obligations, such as maintaining gender-based rosters or other statutory registers. Even if these categories do not explicitly align with 'employment purposes,' they may still be processed under these specific exceptions provided by law.

Citation	Sections 4,5,6, and 7 of the Act

3.4.4. Is it permissible to disclose/share such personal information with third parties?

Please refer to section 2.1.4. and the corresponding questions addressed within that section.

Citation	Sections 2,7, and 8 of the Act

3.5. Payroll and pension records

3.5.1. Is it permissible to process personal information contained in payroll and pension records?

Please refer to section 2.1.1. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, and 7 of the Act

3.5.2. Are there any restrictions on processing such data?

Please refer to section 2.1.2. and the corresponding questions addressed within that section.

Citation	Sections 4, 5, 6, 7, and 8 of the Act

3.5.3. Which lawful bases can be relied on for processing personal information contained in payroll and pension records?

Please refer to section 2.1.3. and the corresponding questions addressed within that section.

Payroll and pension records are an integral part of managing employment-related responsibilities. These records are directly tied to an employer's core obligations, such as paying salaries, maintaining financial records, and fulfilling statutory requirements like tax deductions and Provident Fund contributions. Given their clear link to employment functions, it's reasonable to view these activities as falling under the employment purposes as outlined in Section 7(i) of the Act, where consent from employees may not be necessary.

Additionally, under Section 7(d) of the Act, employers are allowed to process personal data without consent if it is required to meet legal obligations. For example, payroll data is often essential for complying with labor laws or submitting statutory filings to government authorities. Pension records may similarly be needed for statutory purposes, such as handling gratuity or provident funds.

However, when payroll or pension data is used for purposes outside of these core or statutory obligations, such as sharing with third parties for optional financial services, explicit consent from employees is advisable. To avoid any uncertainties and maintain compliance, employers should ensure they adhere

to principles like purpose limitation and data minimization while considering consent for non-essential uses of such data.

Citation	Section 7 of the Act

3.5.4. Is it permissible to disclose/share such personal information with third parties?

Please refer to section 2.1.4. and the corresponding questions addressed within that section.

Citation	Sections 2,7, and 8 of the Act

4. Data subject rights

4.1. Access requests

4.1.1. Are there any specific rules for handling employee access requests?

Section 11 of the Act grants employees, as data principals, the right to request access to specific information related to the processing of their personal data. This right applies only to personal data for which the employee has given explicit consent under Section 6 of the Act or voluntarily provided their data as per Section 7(a) of the Act. Employers acting as data fiduciaries must provide the following upon request.

- A summary of the personal data being processed by the employer and details of the processing activities undertaken.
- Identities of other data fiduciaries and data processors with whom the personal data has been shared, along with a description of the data shared.
- Additional information is prescribed by the rules regarding personal data and its processing. However, as per the Draft Rules, no such additional

information has been prescribed yet. Therefore, this provision remains inoperative until such rules are notified.

It is essential to note that these rights are tied directly to data collected with the consent of the employee or voluntarily shared (Section 7(a) of the Act).

If the processing is authorized under other grounds, such as those under Section 7 of the Act, like employment purposes or compliance with a legal obligation, the employer may not be required to provide this information.

Citation	Sections 5, 6, 7, and 11 of the Act

4.1.2. Are there any limitations to providing employees access to their personal information?

Yes, there are specific limitations to the access rights provided to employees. As per Section 11(2) of the Act, these limitations apply specifically to Section 11(1)(b) and (c) of the Act. This means employers are not obligated to disclose the following.

- Details about data shared with other data fiduciaries or data processors where such sharing is legally authorized. For instance, if the employer shares data with government authorities for investigations or to comply with legal requirements, this disclosure is exempted.
- Additional prescribed information related to the processing of personal data, particularly where such disclosure could interfere with the legitimate functioning of legal mandates or investigative processes.

It is important to note that the limitations under Section 11(2) of the Act do not extend to Section 11(1)(a) of the Act, which grants employees an unqualified right to access a summary of their personal data and its processing activities. Employers must provide this information upon request unless exemptions under Section 17 of the Act apply.

Section 17 of the Act introduces critical exemptions that further shape the scope of employee access rights. For instance, employers can deny access requests if the processing of personal data is necessary for enforcing a legal right or claim. This ensures that access rights do not conflict with ongoing legal obligations or litigation processes.

Citation	Sections 11 and 17 of the Act

4.2. Privacy policies

4.2.1. Is there a requirement to provide employees with a privacy policy?

Although the Act does not explicitly mandate the provision of a privacy policy, the notice requirement under Section 5 of the Act and Rule 3 of the Draft Rules effectively serves the same purpose by informing employees about the processing of their personal data. However, having a formal employee-facing privacy policy can be interpreted as an important step towards compliance with the law and can enhance overall adherence to other requirements of the Act and the Draft Rules.

The Act places ultimate accountability on the employer, even when data breaches or mishandling occur due to employee actions or third-party data processors. Under Section 8(1) of the Act, the employer remains liable for ensuring compliance with the Act, regardless of agreements with employees or external processors. For instance, if an employee provides false personal data or if a third-party processor fails to adhere to the Act's safeguards, the employer may face regulatory consequences. A privacy policy that explicitly communicates employee rights and responsibilities which can help mitigate these risks.

To comply with Section 8(4) of the Act, which requires data fiduciaries to implement appropriate organizational measures, it can be reasonably interpreted that having a comprehensive privacy policy, in principle, aligns with the intended purpose of this requirement. While the Act does not explicitly mandate a privacy policy, its structure and objectives suggest that having one can be deemed essential to effectively meet the obligations under Section 8(4) of the Act, as it provides a clear framework for data-handling practices and ensures employees are informed of their rights as data principals.

Furthermore, Section 15 of the Act outlines specific duties of employees, such as not suppressing material information (Section 15(c) of the Act) and providing only verifiably authentic data (Section 15(e) of the Act). These duties should be reflected in the privacy policy to ensure employees understand

their role in maintaining compliance. For example, if an employee intentionally provides false bank details, the employer could face repercussions for processing inaccurate data. Including these obligations in the policy creates a clear framework, reducing the likelihood of such incidents.

Please note that even if Section 8(4) of the Act is not explicitly interpreted to mandate privacy policies, implementing one is a best practice for the above-mentioned reasons.

Citation	Sections 5, 8, and 15 of the Act

4.2.2. What information must be provided to employees regarding the processing of their personal information?

Please refer to section 4.2.1. above.

Citation	Sections 5, 8, and 15 of the Act

4.2.3. When must this information be provided?

While the law doesn't lay down a specific timeline for sharing the privacy policy (as there is no explicit requirement to have a privacy policy in the first place), it's a good idea to make it available to employees from their very first day on the job. This ensures that employees are aware of their responsibilities from the start, making compliance with the Act easier and more effective.

Citation	Not applicable, author recommendation.

4.2.4. In what format must this information be provided?

The Act doesn't specifically require organizations to have a privacy policy, nor does it provide a set format for one. That said, it's important for organizations to draft their privacy policy in a way that’s clear and easy for employees to understand. A well-structured and straightforward policy can go a long way in helping employees know how their personal data is being handled and what their rights are.

Citation	Not applicable, author recommendation.

5. Use of AI and automated decision-making

5.1. Recruitment

5.1.1. Are there requirements regarding the use of automated decision-making and/or AI during recruitment?

The Act does not explicitly regulate automated decision-making or artificial intelligence (AI) during recruitment. However, the Act's general principles and provisions apply to any personal data processing, including data processed using automated decisions or AI. Below are some key considerations.

Accuracy

Employers, as data fiduciaries, are obligated under Section 8(3) of the Act to ensure that personal data processed during recruitment is accurate, complete, and consistent. This is particularly critical if the data will be used to make decisions affecting candidates or disclosed to another data fiduciary. Therefore, it becomes very important for employers to ensure that data processed by AI and/or automated decision-making is accurate, complete, and consistent.

Contracts with AI vendors (data processors)

If an employer engages an external AI platform for recruitment, the AI vendor acts as a data processor under the Act. As per Section 8(2) of the Act, employers must enter into a valid contract with the data processor, defining the scope and purpose of data processing. Despite such contracts, the data fiduciary (employer) retains ultimate accountability under the Act. Any non-compliance by the AI vendor would result in liability for the employer. Therefore, it must be ensured that the external vendor engaged can be trusted and adheres to the provisions of the Act.

Discrimination risks in AI systems

Employers must ensure that automated decision-making or AI systems used in recruitment are free of bias and comply with anti-discrimination laws, including the below.

- The Equal Remuneration Act, 1976 prohibits discrimination against women in recruitment.
- The Code on Wages, 2019 which is yet to be implemented, expands this prohibition to all genders.

If an AI system ranks candidates unfairly based on gender, it could lead to legal and regulatory challenges. Employers must therefore audit AI systems regularly to mitigate such risks.

Citation	Section 8 of the Act

5.1.2. What are the requirements regarding the use of automated decision-making and/or AI during recruitment?

Please refer to section 5.1.1. above.

Citation	Section 8 of the Act

5.2. Employee performance

5.2.1. Are there requirements regarding the use of automated decision-making and/or AI to evaluate employee performance?

Please refer to section 5.1.1. above.

Citation	Section 8 of the Act

5.2.2. What are the requirements regarding the use of automated decision-making and/or AI to evaluate employee performance?

Please refer to section 5.1.1. above.

Citation	Section 8 of the Act

6. Teleworking

6.1. Policy, procedures, and guidance

6.1.1. Are there any specific requirements for employers with employees that work remotely?

The Act does not specifically address teleworking arrangements. That said, employers must ensure compliance with the general principles of the Act while facilitating teleworking. This includes implementing technical and organizational measures under Section 8(4) of the Act to secure personal data, particularly as employees work remotely.

Moreover, employers should ensure clear contractual arrangements with third-party vendors handling teleworking tools or platforms. Despite such agreements, the ultimate responsibility lies with the employer (data fiduciary), who must bear the consequences of any breach, even if caused by a vendor (data processor).

Citation	Not applicable.

6.1.2. What are the requirements for employers with employees that work remotely?

Please refer to section 6.1.1. above.

Citation	Not applicable.

7. Training and awareness

7.1. Employee training

7.1.1. Are there any requirements for training employees on data protection compliance?

While there is no explicit requirement to train employees on data protection under the Act and the Draft Rules, the same requirements under Section 8(4) of the Act, which provides for appropriate organizational measures, can reasonably be extended to include employee training. For the same reasons outlined in section 4.2. above, such as fostering awareness of data-handling practices, ensuring employees understand their rights and duties, and enabling better compliance with the Act, organizations are strongly encouraged to provide regular training. Training programs can ensure that employees are not only aware of their responsibilities but also equipped to assist the organization in fulfilling its compliance obligations.

Citation	Section 8 of the Act

7.1.2. What should employee training programs encompass?

Please refer to section 7.1.1. above.

Citation	Section 8 of the Act

8. Enforcement

8.1. Liability

8.1.1. What are the penalties for violation of the applicable laws?

The Act imposes severe penalties for violations, holding employers accountable for breaches of data protection obligations as prescribed under the Schedule provided in the Act. The maximum penalty prescribed under the Schedule is INR 2.5 billion (approx. $ 29.30 million).

Citation	Section 33 read with the Schedule of the Act

8.2. Enforcement decisions

8.2.1. Has the supervisory authority issued any enforcement decisions on data protection and employment?

Currently, there are no enforcement decisions issued on data protection and employment given the Act, which will be the governing legislation in this regard, has not yet come into force.

Citation	Not applicable.

8.3. Case law

8.3.1.

Are there any relevant decisions on data protection and employment from judicial courts?

Currently, there are no case laws issued on data protection and employment given the Act, which will be the governing legislation in this regard, has not yet come into force.

Citation	Not applicable.

Topics: Employment

Jurisdictions: India

Related