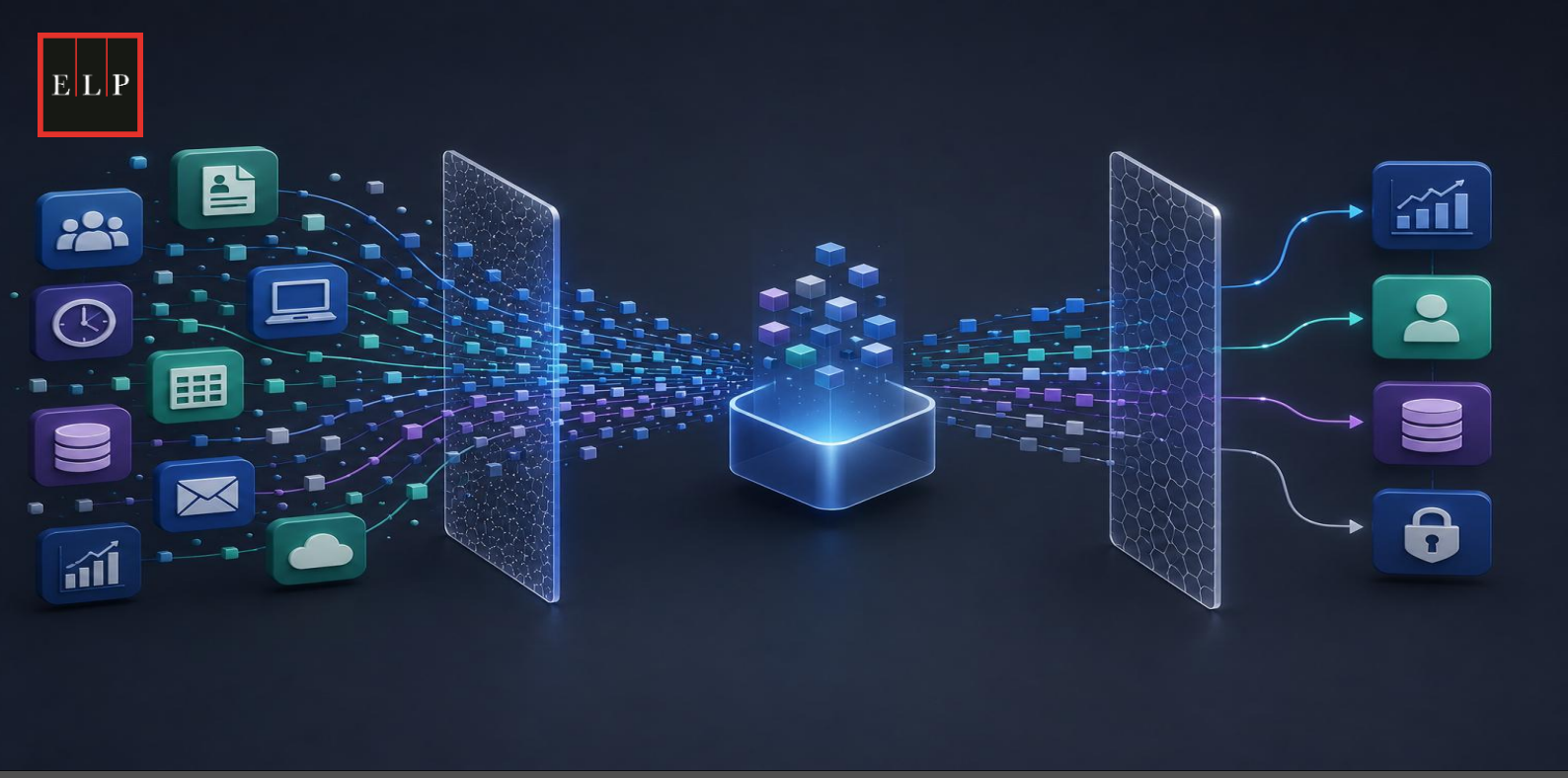

Processing employee-related data: Where are the potential boundaries?

INTRODUCTION

The Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) were notified by the Ministry of Electronics and Information Technology on November 13, 2025, operationalizing the Digital Personal Data Protection Act, 2023 (**DPDP Act**), which will be implemented in a phased manner. Under the DPDP framework, processing of digital personal data (**DPD**) must either be based on a data principal's consent or for certain 'legitimate uses', which are non-consent-based grounds for processing.

One such 'legitimate use' permits an employer to process DPD without consent for (i) purposes of employment; (ii) to safeguard the employer from loss or liability; or (iii) provision of any service or benefit sought by a data principal.

This primer analyses the boundaries of this legitimate use, discussing the possible reliance on this basis for processing, and key considerations for businesses.

PROCESSING DPD FOR PURPOSES OF EMPLOYMENT

- **Moving the needle - purpose "related to employment" to purpose "for employment":** The earlier iterations of the DPDP framework, (*i.e.*, the Personal Data Protection Bills of 2018 and 2019) permitted processing of employee personal data without consent for specific employment-related purposes (including recruitment/ termination, verifying attendance, etc.), where obtaining consent was not appropriate or would be disproportionate. The Personal Data Protection Bill, 2022 marked a shift by deeming consent to have been provided by an employee, if its personal data was being processed for "*purposes related to*" employment, illustratively setting out the purposes (including recruitment/ termination, verifying attendance, assessment of performance, etc.)

  Contrary to the 2022 Bill, the DPDP Act uses the phrase "purposes *of* employment" instead of "purposes *related to* employment". While the preposition "of", depending on the context in which it is used, may denote a relationship between two things,[1] the use of "of" in place of the phrase "related to" likely reflects a legislative intent to require

[1] For example, one of the meanings of the preposition "of" is "related to a thing or person"

a closer nexus[2] between the relevant purpose and employment as compared to the formulation used in the 2022 Bill. Considering this shift, the current framing seems to arguably envisage only such processing that would have a proximate nexus with the employment, as opposed to "any" connection or relationship. The DPDP Act also envisages processing of employee-related data without consent for (i) safeguarding an employer from loss or liability; or (ii) providing any service or benefit sought by the employee, streamlining the grounds under previous iterations.

- **What might be potential scenarios for this legitimate use?:** Given the DPDP Act's foundational principles of protecting DPD, any reliance on "legitimate use" exceptions are likely to be interpreted through the lens of the Supreme Court's *Puttaswamy judgment. Puttaswamy* establishes that while the right to privacy is not absolute, any restriction must meet the three-pronged test.[3] Specifically, any processing of DPD must meet the test of necessity and proportionality. Guided by this framework, certain illustrative scenarios where an employer can process employee-related DPD without consent, on the basis of "legitimate use", are:

  - ***Safeguarding the employer from loss or liability***. An employer can process an employee's DPD for prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, and classified information, without obtaining consent. The objective of this basis for processing appears to be to protect an employer from 'loss' or 'liability', however, what may constitute such 'loss' or 'liability' has not been clarified.
    - For example, if an employer suspects corporate espionage, leakage of confidential data, or theft of intellectual property, it may process suspected employee(s)' DPD for investigating such concerns and for such processing, the employee's consent would not be required.

    Employers must avoid over-reliance on this provision and ideally rely on this provision where 'loss' or 'liability' may be reasonably demonstrable.

  - ***Provision of services or benefits sought by an employee***. An employer can process an employee's DPD to provide any service or benefit sought by an employee, without obtaining consent. This ground appears intended to facilitate processing that is necessary for the employer to provide a service or benefit specifically requested or availed of by the employee.
    - For example, if an employee requests assistance for relocation, including temporary accommodation or travel-related reimbursement, the employer can process the employee's DPD to provide the requested assistance, without obtaining consent.

  - ***For the purposes of employment***. As stated above, this ground for processing seems to draw a closer link between the processing activity and employment. Viewed through such a lens, processing for this purpose would include those activities that are necessary to the employer-employee relationship. Conversely, any processing activity that is unrelated to or not necessary for employment may not pass muster upon closer scrutiny.
    - For example, an employer can process an employee's DPD for salary disbursement, without obtaining consent.

    However, if the purpose of the processing is not necessary, relying on this ground for processing may be disproportionate.
    - For example, an employer sharing employee(s)' DPD with affiliated entities for marketing products/ services could be viewed as not necessary and disproportionate, and would, therefore, require prior consent.

[2] The term "related" means 1. Connected in *some way*; having relation to or with something else". . .", Black's Law Dictionary, 10th Ed. In other words, one could possibly argue that any nexus with employment could be viewed as a purpose related to employment under the 2022 Bill as opposed to a proximate and intrinsic nexus with employment under the DPDP Act because of the usage of the preposition "of".

[3] See, *Justice KS Puttaswamy (retd.) & Anr. v. Union of India*, 2017 SCC OnLine SC 996, at para 325, the Supreme Court laid down the proportionality framework, which includes three elements: (i) existence of law; (ii) necessity, and; (iii) proportionality.

CONSIDERATIONS FOR EMPLOYERS

To ensure that employee-related DPD is processed within the permissible contours of this legitimate use, employers may consider adopting practices such as:

- ***Keep employees informed***. Employers should consider putting in place employee handbooks or HR policies which in turn, among others, set out the type of DPD being collected, the purpose(s) of such collection, and other entities with whom the DPD may be shared along with reasons.
- ***Demarcate employee-related data***. DPD of employees should be clearly mapped and categorized along with the purposes for which such DPD would be processed. Employee-related DPD, that may be processed without consent, should be demarcated from other DPD which requires consent for processing.
- ***Access limitations***. Similar to non-employee DPD, the use of employee-related DPD should be subject to appropriate reasonable safeguards including limited access by stakeholders as may be necessary for stated purposes.
- ***Training relevant teams/ personnel***. As part of internal compliance training with respect to data governance and protection practice, employers should consider emphasizing training relevant stakeholders with respect to handling of employee-related DPD as well to avoid excessive processing.

CONCLUSION

While the DPDP Act permits non-consent-based processing of employee-related DPD, such processing must remain grounded in the core principles of necessity, proportionality, and adherence to the boundaries of the law. Employers must ensure that any reliance on these grounds is carefully assessed, narrowly tailored to a specific employment-related purpose, and supported with appropriate organizational safeguards. Considering the evolving nature of the DPDP framework, employers should adopt a cautious approach and, where the applicability of this legitimate use is unclear, rely on the notice-and-consent framework to mitigate compliance risk.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -ravisekharnair@elp-in.com

Parthsarathi Jha, Partner – Email - parthjha@elp-in.com

Priyanjali Singh, Associate- Email – priyanjalisingh@elp-in.com