# CHECKLIST: PERSONAL DATA PROTECTION LAW

## 1. INTRODUCTION

- The Personal Data Protection Bill, 2019 ("**PDP Bill**") was introduced in Parliament on 11 December 2019. If passed, the law will require organisations to revamp their data-related processes and embed privacy within their systems and operations.
- Accountability is a key feature of the PDP Bill and organisations should be prepared to demonstrate compliance with its requirements. The PDP Bill proposes significant penalties for non-compliance that could go up to 4% of total worldwide turnover of an entity.
- The PDP Bill establishes a new regulator – the Data Protection Authority of India ("**DPA**") – that is entrusted with enforcing this new law and ensuring compliance.
- This checklist is intended to be a starting point for organisations to understand their obligations under the law. The checklist lists out compliance requirements and action items for organisations under five heads: (i) understanding scope and preparing for the law; (ii) accountability; (iii) fair and lawful processing; (iv) data principals' rights; and (v) transferring data outside India. The checklist indicates whether a set of actions is relevant for data fiduciaries (data controllers) ("**DFs**") or data processors ("**DPs**") or both. It also identifies the relevant teams that need to be involved in each set of actions:

| | | | |
|---|---|---|---|
| Legal/ Compliance | 🔴 | Public Relations | 🟠 |
| Technical and IT | 🔵 | HR | 🟡 |
| Customer Relations | 🟢 | | |

## 2. COMPLIANCE CHECKLIST

### (I) UNDERSTANDING SCOPE AND PREPARING FOR THE LAW

| Subject | Description of PDP Bill requirement | Action | Relevant PDP Bill provision |
|---|---|---|---|
| Scope<br>🔴<br>(DF/DP) | The PDP Bill applies to the processing of 'personal data'. Processing means collection, use, storage, sharing or any other activity related to data.<br><br>The PDP Bill regulates data-processing activities of 'data fiduciaries' and 'data processors'. | Organisations should:<br>▪ Identify if they process any personal data (i.e. data that relates to an individual or can identify an individual).<br>▪ Understand if they determine the purpose and means of data processing. If so, they will be data fiduciaries.<br>▪ Understand if they are only processing data on behalf of another entity. In that case, they may be data processors.<br>▪ Identify if their data processing activities are exempted under the law. | Clauses 2, 26 |

| | | | |
|---|---|---|---|
| | 'Significant data fiduciaries' are required to comply with heightened obligations, such as conducting data protection impact assessments, appointing a data protection officer, record-keeping, and having their processes audited yearly. Social media intermediaries are classified as 'significant data fiduciaries' under the PDP Bill. | ▪ Understand if they are 'significant data fiduciaries' (notified by the DPA). | |
| Territorial scope<br><br>(DF/DP) | The PDP Bill applies to data processing in India and to processing by Indian entities.<br><br>The PDP Bill applies to processing outside India if it is in connection with any business carried out in India, or the systematic offering of goods or services in India; or in connection with any activity that involves profiling of data principals in India.<br><br>The central government can exempt certain data processors from the law, where pursuant to contracts with offshore entities, data processors process data of individuals who are outside India. | Organisations should:<br>▪ Identify if any part of their data processing activity takes place in India.<br>▪ If they process data outside India, identify if Indian citizens are involved or if the activity is conducted in connection with any business in India or offering of goods and services in India. | Clauses 2, 37 |
| Data inventory<br><br>(DF/DP) | Significant data fiduciaries are required to keep records of important operations in the data life cycle.<br><br>While not specifically required, several provisions such as privacy by design, data protection impact assessment, etc. will start with the preparation of a data inventory and mapping data flows. An inventory is the first step towards compliance with the PDP Bill. | Organisations should:<br>▪ Identify all data processed and held within different departments, including details such as its source, who it will be shared with, who has access to it within the organisation, etc.<br>▪ Create a comprehensive data inventory using this information.<br>▪ Consider using automated privacy tools for preparing a data inventory.<br>▪ Develop processes for updating the inventory periodically.<br>▪ Understand different types of data with the organisation, such as 'personal data', 'sensitive personal data', 'critical personal data' and 'non-personal data'. | Clause 28 |

| | | | |
|---|---|---|---|
| Non-personal data<br><br>(DF/DP) | While most compliance requirements relate to personal data, data fiduciaries and processors can be asked by the central government to share anonymised or non-personal data for specific policy goals. | Organisations should:<br>• Understand types of non-personal data they hold and process.<br>• Develop processes to respond to government directions for non-personal data. | Clause 91 |

## (II) ACCOUNTABILITY

**Accountability: Governance and Systems**

| Subject | Description of PDP Bill requirement | Action | Relevant PDP Bill provision |
|---|---|---|---|
| Privacy by design policy<br><br>(DF) | Data fiduciaries should prepare a privacy by design policy. They may get this certified by the DPA. Once certified, they will be eligible to participate in a sandbox proposed under the PDP Bill. Through this privacy by design policy, they should embed privacy features in their systems and adopt suitable organisational and technical systems. | Organisations should:<br>▪ Develop a privacy by design policy.<br>▪ Develop procedures to identify risk of harm to data principals and formulate mitigation strategies.<br>▪ Ensure data protection obligations (such as purpose limitation, collection limitation, data quality and data storage) are reflected in business practices and in IT systems.<br>▪ Employ technology that is in accordance with commercially accepted or certified standards.<br>▪ Develop and implement processes to train personnel across all levels to ensure they understand data protection principles and PDP Bill requirements.<br>▪ Ensure privacy features are embedded into all parts of a data life cycle. | Clause 22 |
| Data protection impact assessment<br><br>(DF) | Before undertaking certain processing activities, significant data fiduciaries are required to conduct a data protection impact assessment ("**DPIA**"). The activities for which a DPIA is required: processing involving new technologies or large scale profiling or use of sensitive personal data, or processing which carries | Organisations should:<br>▪ Create internal processes to ensure that privacy risk is understood as a business risk in the development of a product and the appropriate teams are flagged when a product involves an activity that requires a DPIA.<br>▪ Develop processes for conducting DPIAs and assign responsibility to relevant personnel.<br>▪ Develop templates for DPIA reports. | Clause 27 |

| | | | |
|---|---|---|---|
| | a significant risk of harm to data principals.<br><br>(The DPA will decide whether all organisations have to comply with this requirement or only significant data fiduciaries.) | | |
| Security safeguards<br><br>(DF/ DP) | Data fiduciaries should adopt appropriate security safeguards, after considering the nature and purpose of processing, risks associated with the processing, and likelihood and severity of harm that could arise from processing.<br><br>(The DPA may issue standards for security safeguards to be maintained by data fiduciaries and data processors.) | Organisations should:<br>▪ Develop procedures to assess risks associated with processing and the likelihood and severity of harm to individuals from their data-processing activities.<br>▪ Develop procedures to mitigate those risks using appropriate security safeguards.<br>▪ Include appropriate techniques such as de-identification, encryption, identity and access management, data loss prevention, as required.<br>▪ Undertake review of security safeguards periodically.<br>▪ Ensure third party contracts have appropriate security controls.<br>▪ Review security safeguards periodically and maintain a record of the review. | Clause 24 |
| Data audits<br><br>(DF) | Significant data fiduciaries should have their policies and processing activities audited annually by an independent data auditor.<br><br>(The DPA will decide whether all organisations have to comply with this requirement or only significant data fiduciaries.) | Organisations should:<br>▪ Develop processes to enable third party audits.<br>▪ Develop internal processes to demonstrate compliance with obligations under the PDP Bill. | Clause 29 |
| Grievance redressal<br><br>(DF) | Data fiduciaries should have effective grievance redressal mechanisms. | Organisations should:<br>▪ Create mechanisms for data principals to raise grievances with the organisation and receive timely responses.<br>▪ Designate officers who will be the points of contact for such grievances. | Clause 32 |

| | | | |
|---|---|---|---|
| Breach notification<br>  <br>(DF) | Data fiduciaries should notify the DPA of a breach where such breach is likely to cause harm to a data principal. | Organisations should:<br>▪ Develop data breach response procedures to notify the DPA as soon as possible in case of a breach.<br>▪ Put in place procedures to assess situations exposing data principals to risk of harm.<br>▪ Prepare templates for notifying the DPA and data principals (when directed by the DPA).<br>▪ Review contracts with third parties and processors to ensure the fiduciary will be able to notify the DPA in time.<br>▪ Review liability provisions in third party contracts for breaches caused by third parties.<br>▪ Review insurance coverage for data breaches. | Clause 25 |

**Accountability: Personnel**

| **Subject** | **Description of PDP Bill requirement** | **Action** | **Relevant PDP Bill provision** |
|---|---|---|---|
| Personnel<br>  <br>(DF) | While not a specific requirement, several obligations under the PDP Bill require personnel to be adequately trained. For instance, privacy by design requires data fiduciaries to ensure that managerial, organisational and business practices are designed to anticipate and avoid harms to data principals. | Organisations should:<br>▪ Ensure that senior management is aware of the compliance requirements and impact of non-compliance.<br>▪ Allocate budget for data protection compliance.<br>▪ Consider having clear lines of reporting and allocation of responsibility for data governance within the organisation.<br>▪ Implement programmes to train personnel on data protection compliance requirements under the law and concepts such as harm and risk to individuals as a result of processing. | Clause 22 |
| Data protection officer<br>  <br>(DF) | Significant data fiduciaries should appoint data protection officers to ensure compliance with the PDP Bill and act as a point of contact for the data principal and the DPA. | Organisations should:<br>▪ Understand if they are a significant data fiduciary or are otherwise required to appoint a data protection officer.<br>▪ If required, appoint a data protection officer as the point-of-contact for all data compliance related issues.<br>▪ Ensure that the data protection officer resides in India. | Clause 30 |

| | | | |
|---|---|---|---|
| | (The DPA will decide whether all organisations have to comply with this requirement or only significant data fiduciaries.) | | |

### (III) FAIR AND LAWFUL PROCESSING

| Subject | Description of PDP Bill requirement | Action | Relevant PDP Bill provision |
|---|---|---|---|
| Basis for processing personal data<br>🔴 🟢<br>(DF) | Any processing should be conducted under one of the legal bases/ grounds specified. These include consent, state action, legal obligation, compliance with court order, emergencies, employment and reasonable purposes to be specified by the DPA. | Organisations should:<br>▪ Identify and document a legal basis for processing any category of data.<br>▪ Before relying on consent, understand if any of the other bases are applicable. For instance, if personal data has to be shared under a law or for compliance with a court order, separate consent would not be required.<br>▪ Explain the bases of processing in their privacy policies/ notices. | Chapter III |
| Consent<br>🔴 🟢 🔵<br>(DF) | In order to lawfully process personal data, data fiduciaries must comply with strict consent requirements. They should obtain consent that is informed, free, clear and specific. In case of sensitive personal data, obtain 'explicit' consent. | Organisations should:<br>▪ Ensure that consent is sought before processing.<br>▪ Determine what makes consent 'explicit'.<br>▪ Maintain clear records of consent obtained from data principals to be able to demonstrate that consent was given at the time of processing.<br>▪ Ensure that provision of goods or services or performance of a contract is not conditional on consent to processing any personal data that is not necessary for that purpose.<br>▪ Ensure that consent is free, specific and clear.<br>▪ Review existing consents to ensure compliance with the new requirements and where non-compliant, draft new consent forms to seek fresh consent.<br>▪ Create mechanisms to allow data principals to withdraw consent.<br>▪ Create mechanisms to allow data principals to give or withdraw consent through consent managers. | Clauses 11, 23 |
| Privacy notice<br>🔴 🔵 🟢 | Data fiduciaries should notify data principals of: type of data collected, manner of collection, purpose of | Organisations should:<br>▪ Review and update privacy notices to make them PDP Bill-compliant (or develop privacy notices where they do not exist). | Clauses 7, 23 |

| | | | |
|---|---|---|---|
| (DF) | collection, likelihood of significant harm, procedure for exercise of data principal rights, among other things. | ▪ Develop processes to provide information in a clear and easily comprehensive form. | |
| 'Reasonable purpose' as a legal basis for processing<br>  <br>(DF) | Data fiduciaries can process personal data if the processing is necessary for 'reasonable purposes' specified by the DPA These may include mergers and acquisitions, network and information security, debt-recovery and fraud prevention. | Organisations should:<br>▪ Understand if processing is for any of the reasonable purposes specified by the DPA.<br>▪ Assess whether processing is 'necessary' for a listed reasonable purpose, having regard to factors such as interest of the data fiduciary in that processing, any public interest in processing, and the reasonable expectation of the data principal with respect to the processing.<br>▪ Record the assessment to be able to demonstrate compliance. | Clause 14 |
| Children's data<br>  <br>(DF) | Data fiduciaries should process children's personal data in a manner that protects their interests and implement appropriate mechanisms for age verification and parental consent. The DPA may designate certain data fiduciaries who processing large volumes of data relating to children as 'guardian fiduciaries' | Organisations should:<br>▪ Identify proportion of personal data likely to be of children and assess possibility of harm to children arising out of processing.<br>▪ Develop appropriate methods to verify age.<br>▪ Create forms for seeking parental consent. | Clause 16 |

### (IV) DATA PRINCIPALS' RIGHTS

| Subject | Description of PDP Bill requirement | Action | Relevant PDP Bill provision |
|---|---|---|---|
| Right to confirmation and access<br>  <br>(DF) | Data fiduciaries should provide clear and concise confirmation and summary of personal data processing activities and the list of data fiduciaries with whom the personal data has been shared. | Organisations should:<br>▪ Develop processes to allow individuals to make such requests.<br>▪ Create templates for summaries of personal data and processing activities to be provided to data principals, upon request.<br>▪ Consider automated means to provide confirmation and summary of processing activities to data principals.<br>▪ Maintain a list of entities with whom the personal data of is shared. | Clause 17 |

| | | | |
|---|---|---|---|
| Right to seek correction<br>  <br>(DF) | Data fiduciaries should enable data principals to seek rectification or completion of their personal data. | Organisations should:<br>▪ Develop internal processes that enable correction of inaccurate data, completion of incomplete data, and update old data in a timely manner.<br>▪ Create a system whereby relevant stakeholders are notified of any change to the data pursuant to such requests.<br>▪ Understand the legal mechanisms under which these rights can be resisted.<br>▪ Develop templates which list the reasons for denial of such requests. | Clause 18 |
| Right to data portability<br>  <br>(DF) | Data fiduciaries should provide and transmit personal data collected through automated means to a data principal or another data fiduciary in a machine-readable format. | Organisations should:<br>▪ Classify personal data according to automated processing and non-automated processing.<br>▪ Assess different machine-readable formats.<br>▪ Develop processes to enable secure data transfer to other data fiduciaries.<br>▪ Understand the legal mechanisms under which such requests can be resisted. | Clause 19 |
| Right to be forgotten<br>  <br>(DF) | Data fiduciaries should restrict or prevent disclosure of personal data of individuals, if required to do so by the adjudicating officer. | Organisations should:<br>▪ Develop processes to determine the relevance of the data to the purpose of collection.<br>▪ Inform other stakeholders that the data principal has requested the erasure of personal data. | Clause 20 |

### (V) TRANSFERRING DATA OUTSIDE INDIA

| **Subject** | **Description of PDP Bill requirement** | **Action** | **Relevant PDP Bill provision** |
|---|---|---|---|
| Data localisation<br>  <br>(DF/DP) | Data fiduciaries should: (i) store sensitive personal data in India (but they can transfer such data outside India under limited legal bases); (ii) store and process critical personal data only in India. | Organisations should:<br>▪ Identify where data resides and review the residency practices.<br>▪ Ensure local processing and storage of critical personal data.<br>▪ Ensure local storage of sensitive personal data. | Clause 33 |

| | | | |
|---|---|---|---|
| Cross-border transfers<br><br>(DF/DP) | Data fiduciaries may transfer sensitive personal data outside India under limited bases, which include: contract/ intra-group transfers approved by the DPA; transfers to countries/ sectors with adequate protection (permitted by the central government); or transfers specifically approved by the DPA. Transfers would also require explicit consent of the data principal as a necessary precondition. | Organisations should:<br>▪ Review processes for cross-border transfers.<br>▪ Develop specific processes to conduct transfer of sensitive personal data.<br>▪ Ensure that explicit consent is obtained before transferring data outside India.<br>▪ Prepare contracts/ intra-group schemes and have them approved by the DPA.<br>▪ Consider preparing a template for request for specific approval from the DPA.<br>▪ Formulate country-specific processes for cross-border transfers. | Clause 34 |

This checklist is intended as an overview of key action items for compliance with the personal data protection law. This should not be construed as, or relied upon, as legal or professional advice.

**ABOUT IKIGAI LAW**

Ikigai Law is a law and policy firm sharply focused on technology and innovation. We specialize in representing technology businesses, investors, and start-ups, to more mature companies focused on new business models. We work with our clients on regulatory and policy issues, private equity and venture capital investment transactions, mergers and acquisitions and other commercial transactions, intellectual property, and disputes. Our work is at the intersection of law, policy, regulation, technology and business, engaging with key issues such as data protection and privacy, fin-tech, online content regulation, platform governance, digital competition, digital gaming, cloud computing, net neutrality, health-tech, blockchain and unmanned aviation (drones), among others. Our key awards and recognitions include:

- Recognised TMT Practice – Chambers and Partners
- Boutique Law Firm of the Year 2019 – Asian Legal Business
- Law Firm of the Year – Mid Size 2019 by Idex Legal
- "Influential, knowledgable and effective" – Legal500
- Best Legal Advisor to Startups 2019 by Idex Legal

***