

Contractual Arrangements Under India's New Data Protection Law: A Data Fiduciary's Guide to the Data Processing Universe

Background

Under India's new Digital Personal Data Protection Act, 2023 (the "**DPDP Act**"), entities which process any personal data in digital form will be required to implement appropriate technical and organizational measures to ensure compliance. In addition, entities will remain responsible for protecting such data as long as it remains in their possession or under their control, including in respect of separate processing tasks undertaken by data processors on their behalf. These overarching responsibilities will extend to taking reasonable security safeguards and procedures to prevent data breaches, as well as complying with prescribed steps if and when a breach does occur.

Importantly, compared to its predecessor draft and unlike the General Data Protection Regulation ("**GDPR**") of the European Union which places direct regulatory obligations on data processors, the DPDP Act appears to attribute sole responsibility upon the main custodians of data vis-à-vis the individuals related to such data – as opposed to a mechanism of 'joint and several' or shared liability with contracted data processors – *even when* the actual processing may be undertaken by the latter pursuant to a contract or other processing arrangement.

This position appears to be based on the principle that an entity which decides the purpose and means of processing should be held primarily accountable in the event of a personal data breach. Such liability may also be invoked when an event of non-compliance arises on account of the negligence of a data processor. While processing tasks can be delegated to a third party, such delegation and/or outsourcing needs to be made under a valid contract in specified cases.

Further, organizations need to ensure that their own compliance requirements and other statutory obligations remain mirrored in their supply chain in terms of (i) implementing appropriate technical and organizational measures, as well as (ii) taking reasonable security safeguards to prevent a personal data breach. This parallel compliance regime will extend to the actions and practices of data processors, including in terms of rectifying or erasing data. For example, when an individual withdraws a previously issued consent with respect to the processing of personal data for a specified purpose, all entities processing their data – including contracted data processors – must stop, and/or must be made to stop, the processing of such information – failing which the primary entity may be held liable.

Contractual Arrangements

Although the term ‘processing,’ as defined in the DPDP Act, involves automated operations, such operations can be either fully or partially automated. Besides, the definition includes any activity among a wide range of operations that businesses routinely perform on data, including the collection, storage, use and sharing of information. Thus, even those business operations which involve some amount of human intervention and/or stem from human prompts will be covered under the definition of ‘processing,’ and thus, the DPDP Act will remain applicable in all such cases.

A “**data fiduciary**” (*i.e.*, those entities which determine the purpose and means of processing personal data, including in conjunction with other entities) can engage, appoint, use or otherwise involve a data processor to process personal information on its behalf for any activity related to the offering of goods or services to “**data principals**” (*i.e.*, specifically identifiable individuals to whom the personal data relates) as long as it is done through a valid contract. However, irrespective of any agreement to the contrary, a data fiduciary will remain responsible for complying with the provisions of the law, including in respect of any processing undertaken on its behalf by a data processor.

Due Diligence and Risk Assessment

Given that data fiduciaries may be ultimately responsible for the omissions of data processors, contracts between such entities need to be negotiated carefully. In this regard, the risks associated with such outsourced data processing activities need to be taken into account by data fiduciaries, including in respect of risks related to the following categories:

1. **Compliance:** where obligations under the DPDP Act with respect to implementing appropriate technical and organizational measures, preventing personal data breach and protecting data are not adequately complied with by a data processor;
2. **Contractual:** where a data fiduciary may not have the ability to enforce the contract;
3. **Cybersecurity:** where a breach in a data processor’s information technology (“IT”) systems may lead to potential loss, leak or breach of personal data;
4. **Legal:** where the data fiduciary is subjected to financial penalties due to the negligence or omission of the data processor; and
5. **Operational:** arising due to technology failure, fraud, error, inadequate capacity to fulfill obligations and/or to provide remedies.

Thus, data fiduciaries need to (1) exercise due diligence, (2) put in place sound and responsive risk management practices for effective supervision, and (3) manage the risks arising from outsourced data processing activities. Accordingly, data fiduciaries need to select data processors based on a comprehensive risk assessment strategy.

A data fiduciary may need to retain ultimate control over the delegated data processing activity. Since such processing arrangements will not affect the rights of an individual data principal against the data fiduciary – including in respect of the former’s statutory right to avail of an effective grievance redressal mechanism

under the DPDP Act – the responsibility of addressing such grievances will rest with the data fiduciary itself, including in respect of the services provided by the data processor.

If, on the other hand, a data fiduciary outsources its grievance redressal function to a third party, it needs to provide data principals with the option of accessing its own nodal officials directly (*i.e.*, a data protection officer, where applicable, or any other person authorized by such data fiduciary to respond to communications from a data principal for the purpose of exercising their rights).

In light of the above, before entering into data processing arrangements, a data fiduciary may want to have a board-approved processing policy which incorporates specific selection criteria for: (i) all data processing activities and data processors; (ii) parameters for grading the criticality of outsourced data processing; (iii) delegation of authority depending on risks and criticality; and (iv) systems to monitor and review the operation of data processing activities.

Data Processing Agreement

The terms and conditions governing the contract between the data fiduciary and the data processor should be carefully defined in written data processing agreements (“**DPAs**”) and vetted by the data fiduciary’s legal counsel for legal effect and enforceability. Each DPA should address the risks and the strategies for mitigation. The agreement should also be sufficiently flexible to allow the data fiduciary to retain adequate control over the delegated activity and the right to intervene with appropriate measures to meet legal and regulatory obligations. In situations where the primary or initial interface with data principals lies with data processors (*e.g.*, where data processors are made responsible for collecting personal data on behalf of data fiduciaries), the nature of the legal relationship between the parties, including in respect of agency or otherwise, should also be made explicit in the contract. Some of the key provisions could incorporate the following:

- Defining the data processing activity, including appropriate service and performance standards;
- The data fiduciary’s access to all records and information relevant to the processing activity, as available with the data processor;
- Providing for continuous monitoring and assessment by the data fiduciary of the data processing activity, so that any corrective measures can be taken immediately;
- Ensuring that controls are in place for maintaining the confidentiality of customer data, and incorporating the data processor’s liability in case of a security breach and/or a data leak;
- Incorporating contingency plans to ensure business continuity;
- Requiring the data fiduciary’s prior approval for the use of sub-contractors for all or part of a delegated processing activity;
- Retaining the data fiduciary’s right to conduct an audit of the data processor’s operations, as well as the right to obtain copies of audit reports and findings made about the data processor in conjunction with the contracted processing services;

- Adding clauses which make clear that government, regulatory or other authorized person(s) may want to access the data fiduciary's records, including those that relate to delegated processing tasks;
- In light of the above, adding further clauses related to a clear obligation on the data processor to comply with directions given by the government or other authorities with respect to processing activities related to the data fiduciary;
- Incorporating clauses to recognize the right of the data fiduciary to inspect the data processor's IT and cybersecurity systems;
- Maintaining the confidentiality of personal information even after the agreement expires or gets terminated; and
- The data processor's obligations related to preserving records and data in accordance with the legal and/or regulatory obligations of the data fiduciary, such that the data fiduciary's interests in this regard are protected even after the termination of the contract.

Learnings from the GDPR

Many companies that primarily act as data processors have standard DPAs which they ask data fiduciaries to agree to, or negotiate from. The GDPR provides a set of requirements for such DPAs, including certain compulsory information. In India, such standards could evolve through practice, such as by including clauses in DPAs related to the following:

- Information about the processing, including its: (i) subject matter; (ii) duration; (iii) nature; and purpose
- The types of personal data involved
- The categories of data principals (e.g., customers of the data fiduciary)
- The obligations of the data fiduciary

A DPA in India could also set out the obligations of a data processor, including those that require it to:

- Act only on the written instructions of the data fiduciary
- Ensure confidentiality
- Maintain security
- Only hire sub-processors under a written contract, and with the data fiduciary's permission
- Ensure all personal data is deleted or returned at the end of the contract
- Allow the data fiduciary to conduct audits and provide all necessary information on request
- Inform the data fiduciary immediately if something goes wrong

- Assist the data fiduciary, where required, with respect to: (i) facilitating requests from data principals in exercise of their statutory rights; (ii) maintaining security; (iii) data breach notifications; and (iv) data protection impact assessments and audits, if required.

Can a DPA be Used to Transfer Liability?

Even if a personal data breach or an incident of non-compliance arises on account of a data processor's act or omission, a DPA alone may not be sufficient to relieve the corresponding data fiduciary of its obligations (including in terms of a financial penalty, as may be imposed by the Data Protection Board of India (the "DPBI")). However, a DPA may be negotiated such as to allow the data fiduciary to recover money from the data processor in some circumstances.

To be sure, if a data processor fails to comply with its contractual obligations under a DPA and thereby causes a data breach or leads to some other ground of complaint under the DPDP Act, the data fiduciary may still be required to pay the penalty, if and when imposed by the DPBI. However, if such breach and/or non-compliance occurs because the data processor did (or did not do) something, thus amounting to a breach of its DPA with the data fiduciary, then the data fiduciary may be able to seek compensation from the data processor for a breach of the DPA and/or invoke the indemnity provisions under such contract.

For example, a DPA can include a "hold harmless" clause. Such clauses may serve to govern how liability falls between the parties. On the other hand, a limitation (or exclusion) of liability clause may aim to limit the amount that one party will pay to the other in the event that it breaches the contract.

What if a Data Processor Processes Personal Data Outside the Confines of a DPA?

If a data processor processes personal data beyond what is permitted under a DPA, or does so contrary to the data fiduciary's directions, such processor may become a data fiduciary by itself (other than possibly being in breach of the DPA). As long as a data processor operates pursuant to the instructions of a data fiduciary, it is only the latter that will remain directly responsible to data principals under the DPDP Act (for the specified purpose with respect to the processing of such personal data). However, as soon as a data processor determines the means and purpose of processing in its own right, it may become directly responsible to corresponding data principals.

In this regard, a data fiduciary may wish to include a clause in the DPA that obliges the data processor to process personal data only in accordance with the DPA, and to the extent necessary, for the purpose of providing the services contemplated under such DPA. Alternatively, a data processor could be permitted to process personal data further to the written instructions of corresponding data principals. Further, processing outside the scope of the DPA could require a prior contract between the data principal(s) concerned and the data processor, respectively, with respect to a separate arrangement.

Nevertheless, the personal information that a data processor receives from a data fiduciary for the purpose of processing, or that it collects on the latter's behalf, can only be processed pursuant to the restrictions of a DPA. If the data processor starts processing such personal data outside the confines of a DPA, e.g., by gathering additional personal data that it has *not* been instructed to collect, or starts processing data in a way that is inconsistent with, or contrary to, the data fiduciary's directions, such data processor is likely to be considered a data fiduciary for the purposes of the DPDP Act.

Indemnification

As mentioned above, data fiduciaries may need to include indemnity clauses in their DPAs with data processors, where data processors agree to indemnify the data fiduciary against all third-party complaints, charges, claims, damages, losses, costs, liabilities, and expenses due to, arising out of, or relating in any way to a data processor's breach of contractual obligations. A mutual "hold harmless" clause is one in which the protections offered and/or excluded are reciprocal between the parties.

Confidentiality and Security

Data fiduciaries need to ensure the security and confidentiality of customer information which remains in the custody or possession of a data processor. Accordingly, the access to customer information by the staff of the data processor should be strictly on a 'need-to-know' basis, *i.e.*, limited to such areas and issues where the personal information concerned is necessary to perform a specifically delegated processing function.

Further, the data processor should be able to isolate and clearly identify the data fiduciary's customer information to protect the confidentiality of such individuals. Where the data processor acts as a processing agent for multiple data fiduciaries, there should be strong safeguards (including via encryptions of customer data) to avoid the co-mingling of such information related to different entities.

Nevertheless, a data fiduciary should regularly monitor the security practices of its data processors, and require the latter to disclose security breaches and/or cybersecurity-related incidents, including, in particular, a personal data breach. After all, a data fiduciary is required to notify the DPBI as well as each affected individual if a personal data breach occurs. In addition, cybersecurity incidents also need to be reported to the Indian Computer Emergency Response Team ("**CERT-In**") within six hours from the identification or notification of such incident. At any rate, the data processor must be obliged through a DPA to notify the data fiduciary about any breach of security or leak of confidential information related to customers or other individuals as soon as possible.

Business Continuity and Disaster Recovery

Data processors could be required to establish a framework for documenting, maintaining and testing business continuity and recovery procedures arising out of any data processing activity. The data fiduciary could then ensure that the data processor periodically tests such continuity and recovery plans. Further, a data fiduciary could consider conducting occasional joint exercises with its data processors for the purpose of testing such procedures periodically.

To mitigate the risk of an unexpected DPA termination or the liquidation of a data processor, the data fiduciary should retain adequate control over the data processing activities and retain its contractual right to intervene with appropriate measures to continue business operations and customer services. As part of its contingency plans, the data fiduciary may also want to consider the availability of alternative data processors, as well as the possibility of bringing back the outsourced processing activity in-house, especially in the event of an emergency. In this regard, the data fiduciary may need to assess upfront the cost, time and resources that would be involved in such an exercise.

In the event of a DPA termination, where the data processor deals with the data fiduciary's customers directly, the fact of such termination should be adequately publicized among a data fiduciary customers to ensure that they stop dealing with the concerned data processor.

Conclusion

As discussed in our previous [note](#), organizations need to check whether and to what extent the DPDP Act applies to them and their operations. Although the provisions of the DPDP Act are not effective as yet, organizations may need to improve their IT and cybersecurity systems to meet new compliance requirements. Relatedly, organizations should monitor entities in their supply chains, such as suppliers and vendors, about data processing obligations. Further, existing contractual arrangements may need to be reviewed, and future contracts with data processors must be negotiated in light of the DPDP Act's compliance requirements.

*This insight has been authored by **Deborshi Barat** (Counsel); he can be reached at d Barat@snrlaw.in for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

© 2023 S&R Associates

NEW DELHI

64 Okhla Industrial Estate
Phase III
New Delhi 110 020
Tel: +91 11 4069 8000

MUMBAI

One World Center, 1403 Tower 2 B
841 Senapati Bapat Marg, Lower Parel
Mumbai 400 013
Tel: +91 22 4302 8000