September 30, 2018

Joint Secretary
Ministry of Electronics & Information Technology (MeitY)
Room No. 4016
Electronics Niketan
6 CGO Complex
Lodhi Road
New Delhi 110001

Sub: Suggestions and recommendations by PSA on selective clauses of the proposed Personal Data Protection Bill 2018

Dear Sir/Madam,

The Committee of Experts on Data Protection under the Chairmanship of Justice B.N. Srikrishna submitted its report "*A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*" and the draft Personal Data Protection Bill, 2018 on July 27, 2018 ("**DPB 2018**").

Pursuant to MeitY opening the DPB 2018 for public comments, PSA, a full service law firm with offices in New Delhi and Chennai, having substantial experience and expertise in privacy, data protection and information technology laws, proposes certain changes to selected clauses of DPB 2018 (*as discussed in "Recommendations" below*).

PSA's legal team is dynamic, driven, devoted and makes it its business to know the clients' business, possesses sound legal acumen, expertise and knowledge base and is trained to think out of the box and resolve complex legal challenge. The firm is exposed to both Western and Indian cultures and capable of bridging the "business cultural" gaps in negotiations. We provide cost-effective, expeditious and outstanding client service. Owing to our first hand involvement in advising start-ups, IT/ITES MNCs, ERP companies, global information centres, and process outsourcing entities on a wide array of matters, we are hopeful that our suggestions will add value and benefit MeitY in streamlining fundamental aspects of DPB 2018, which will ensure that the future legislation is well attuned with its objectives of creating a "*collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation*."

Yours sincerely,

Arya Tripathy, Principal Associate
For and on behalf of ***PSA***
Tel: +91.11.4350-0500; e-mail: a.tripathy@psalegal.com

RECOMMENDATIONS

I. *Inclusion of lawful contract as a ground for personal data processing*

I.1 Chapter II of DPB 2018 deals with grounds of processing personal data, and draft Section 12 captures consent as its primary basis. Section 12 states:

"*(1) Personal data may be processed on the basis of the consent of the data principal, given no later than at the commencement of processing.*

(2) ……

(3) The data fiduciary shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose.

(4) ……

(5) Where the data principal withdraws consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, all legal consequences for the effects of such withdrawal shall be borne by the data principal."

I.2 *Analysis:*

I.2.1 For consent to be informed and specific (i.e. all information as per draft Section 8 was provided and the data principal is capable to determine the scope of consent), the data fiduciary must specifically mention the purposes for which personal data is to be processed, the source of personal data collection, and whom such personal data will be shared **=>** meaning that

- All purposes, including the purposes which can be reasonably expected by the data principal must be identified to the extent possible, and processing for any other purpose cannot be backed by informed and specific consent theory. Whether a purpose is reasonably expected by the data principal is subjective, and likely to be coloured significantly by her right to informational privacy. It will not objectively factor data fiduciary's requirement to process personal data for fulfilling/performing his contractual obligation *vis-à-vis* the data principal (*like sharing of address details by e-com retailer with aggregator, followed by aggregator with logistics partner for seamless delivery of goods*).

- Further, new consent will be required for processing personal data for a different yet related purpose (*like sharing of contact details by car retailers to car insurers*).

- To top this, repurposing of any kind will be a prohibited act even though such reprocessing may not cause or create likelihood of "harm"[1] or "significant harm"[2] for

[1] Draft section 3(21) defines "harm" to include (i) bodily or mental injury, (ii) loss, distortion or theft of identity, (iii) financial loss or loss of property, (iv) loss of reputation, or humiliation, (v) loss of employment, (vi) any discriminatory treatment, (vii) any subjection to blackmail or extortion, (viii) any denial or withdrawal of a service, benefit of good resulting from an evaluative decision about the data principal, (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal

the data principal, and such approach will stifle several sectors like IT/ITES, Big Data, e-commerce, or any other entity that is reliant on data analytics for its operations.

- In the same vein, where processing activities involve different data processing entities, consent will be required every time there is change in the involved entities, although there is no change in the already notified scope of processing that will be performed by such changed processing entity.

- The data principal has absolute discretion and several disputes are likely to arise on whether (i) data principal consented to a particular purpose and processing, and (ii) the purpose or processing not specifically consented to is reasonable from data principal's perspective. In such disputes, the burden of proof will be on data fiduciary and determination will be a question of fact, leaving the data fiduciaries and processors without any other legal ground to justify a processing or purpose which is related, ancillary or completely new.

I.2.2 At the same time, consent has to be free, specific, clear and capable of being withdrawn. Further, consent cannot be conditional on provision of goods or services or performance of contract i.e. consent for processing of personal data cannot be *per se* the counter-performance of the contract. Furthermore, data principal has a right to withdraw consent, and where withdrawn, all legal consequences flowing there from shall be borne by her **=>** which means that

- While consent cannot be a condition for goods or services and rightly so (as it is an essential for contract conclusion), denial of goods or services due to withdrawal of consent is legal and permissible if it can be shown that processing of personal data was fundamental for provision of goods or services.

- This in effect nullifies the prohibition under draft Section 12(3) and indirectly makes delivery of goods or services conditional on consent, thereby striking at the core of "free consent" and Section 14 of the Indian Contract Act, 1872.

I.2.3 In addition to this and on a joint reading of draft Sections 8[3], 12 and 30,[4] (i) data principal's consent should be 'clear' through an affirmative action in the given context, and (ii) data fiduciary in order to comply with transparency principle must periodically provide information about processing to the data principal **=>** which logically suggests that

- Every time periodic notice is sent concerning processing details, there will be variation in what was originally informed to the data principal under Section 8 notice.

[2] Draft section 3(37) defines "significant harm" to mean harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm

[3] Draft section 8 mandates the data fiduciary to provide enlisted information to the data principal no later than at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable

[4] Draft section 30 mandates the data fiduciary to maintain transparency by taking reasonable steps in retaining enlisted information and providing periodic notice to the data principal

- Accordingly, data fiduciaries must ensure that the data principal's consent is continual and still valid despite the change in information from the original notice.

- This cannot be inferred impliedly as consent must be through an affirmative action, thereby making it indirectly mandatory for the data fiduciary to obtain repeated consents on every notice occasion.

I.2.4 Consent as the only ground for processing of personal data as discussed above raises multiple concerns. Such an approach will impose enormous burden on data fiduciaries that have to maintain valid consents all throughout the data life cycle management. At the same time, consent or click fatigue is a real phenomenon, which will defeat the basic edifice of processing personal data under DPB 2018.

I.3 *Recommendation*

In order to avoid the aforementioned concerns, we recommend that a new Section 13 should be added to DPB 2018 wherein processing of personal data must be held valid, if processing is necessary for

- the performance of a lawful contract to which the data principal is a party;
- performing such actions that is required to enter into a contract with the data principal only when such actions are provided in writing to the data fiduciary by the data principal.

Drawing clue from Article 6(1)(b) of EU General Data Protection Regulation, the language for proposed Section 13 can read as follows:

"*13. Processing of personal data on the basis of a valid contract.-*

Personal data maybe processed if processing is necessary-
(a) for the performance of a lawful contract to which the data principal is party or beneficiary; or
(b) in order to take steps or perform actions at the request of the data principal in writing which are essential for the data principal to enter into a lawful contract with the data fiduciary."

II. *Revisiting data principal's right to be forgotten*

II.1 Chapter VI of DPB 2018 deals with data principal rights, and draft Section 27 captures data principal's right to be forgotten. It states

"*27. Right to be forgotten -*

(1) The data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal where such disclosure –
(a) has served the purpose for which it was made or is no longer necessary;
(b) was made on the basis of consent under Section 12 and such consent has since been withdrawn; or

(c) was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.

(2) Sub-section (1) shall only apply where the Adjudicating Officer under Section 68 determines the applicability of clause (a), (b) or (c) of sub-section (1) and that the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen.

(3) …….

(4) ……..

(5) ……."

II.2 *Analysis*

II.2.1 The right to be forgotten does not capture right to erasure as determined to be the crux in European Court of Justice decision in *Google Spain case*,[5] where it was highlighted that right to seek erasure of data which no longer is relevant is fundamental aspect of informational privacy and truly essential for an individual to exercise control over her personal data. It is limited to preventing or restricting disclosure, subject to adjudication by the Adjudicating Officer. Further, the right can only be exercised if the data principal's right to be forgotten overrides the right to freedom of speech and expression and the right to information of any citizen **=>** which means that

- Where personal data is no longer relevant for the purpose, it cannot be deleted even though there is no obligation on the data fiduciary to maintain quality of such personal data under draft Section 9 that obligates the data fiduciary to take reasonable steps for ensuring that personal data processed is complete, accurate, not misleading and updated having regard to the purpose.

- Once personal data becomes irrelevant *vis-à-vis* the purpose, there is no obligation on data fiduciary to anonymize or de-identify such personal data, and in absence of corollary requirements to this effect, the data principal can be subjected to evaluative decision making which can cause "harm", as happened in *Google Spain case.*

- The right to freedom of speech and expression and the right to information of any citizen cannot be interpreted to mean that an individual has a right to have access and know other individuals' personal data without any mandate under law or judicial order. Where such legal mandate requires disclosure or sharing of personal data, data fiduciary is separately authorised to make such disclosures under DPB 2018, and hence, freedom of speech and expression or right to information cannot be the basis of denying a data principal from her right to seek erasure, continual disclosure and onward sharing.

[5] Google Spain SL, Google Inc. vs. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez Case C-131/12 decided on May 13, 2014 by European Court of Justice (Grand Chamber)

- The Committee believes that in a processing regime driven by consent, there is no need for separately providing the data principal with a right to erasure. The rationale is that processing will cease to the extent consent is withdrawn. Consequently, when consent is withdrawn, the data fiduciary or processor cannot carry any processing operation without consent, including storage, erasure or deletion as these are included within the ambit of "processing" under DPB 2018. Hence, there is an inherent inconsistency where even after consent has been withdrawn, the data fiduciary or processor will in the least continue to store personal data. Absence of the right to seek erasure of personal data thus becomes of extreme importance where the data principal after withdrawing consent can require the data fiduciary or processor to delete her personal data.

- This right will strengthen the principles of fair and reasonable processing, enhance transparency and augment privacy by design through data minimization.

II.3 *Recommendation*

It is imperative that right to forgotten is not restricted to disclosure or sharing, but must also include the right of data principal to seek erasure of data on the conditions mentioned in draft Section 27. The anticipation that this right can be misused by the data principal is without any basis, since the right can only be exercised after adjudication by the Adjudicating Officer, which means that there are adequate checks and balances. Therefore, we recommend that Section 27 is amended in the following manner:

"*27. Right to be forgotten –*

(1) The data principal shall have the right to obtain erasure or restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal where such the personal data processed in any manner –

(a) has served the purpose for which processing performed is no longer necessary;
(b) was made on the basis of consent under Section 12 and such consent has since been withdrawn; or
(c) was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.

(2) Sub-section (1) shall only apply where the Adjudicating Officer under Section 68 determines the applicability of clause (a), (b) or (c) of sub-section (1) having regard to

(a) the sensitivity of the personal data;
(b) the scale of processing and the degree of accessibility sought to be restricted or prevented;
(c) the role of data principal in public life;
(d) the relevance of personal data to the public;
(e) the right to freedom of speech and expression and the right to information of any citizen;
(f) the nature of processing and activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities would be significantly impeded if erasure or disclosure of relevant nature were to be restricted or prevented.

(3) The right under sub-section (1) shall be exercised by filing an application in such form and manner as may be prescribed.

(4) Where any person finds that personal data, the erasure or disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2) does not satisfy the conditions referred to in that sub-section any longer, they may apply for the review of the order to the Adjudicating Officer in such manner as may be prescribed, and such Adjudicating Officer shall review her order on the basis of the considerations referred to in sub-section (2)."

III. *Transparency and accountability measures*

III.1 Chapter VII containing draft Sections 29 to 39 provide the transparency and accountability measures that must be complied by data fiduciaries. Sections 29 to 37 and Section 39 dealing with privacy by design, transparency, security safeguards, personal data breach, data protection impact assessment, record-keeping, data audits, data protection officer, processing by entities other than data fiduciaries, and grievance redressal are worded in such manner that every data fiduciary gets covered, without regard to whether the fiduciary is classified as significant data fiduciary or not. At the same time, Section 38 referring to significant data fiduciaries states:

"*38. Classification of data fiduciaries as significant data fiduciaries –*

(1) The Authority shall, having regard to the following factors, notify certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries –

(a) volume of personal data processed;
(b) sensitivity of personal data processed;
(c) .....

(2) .....

(3) All or any of the following obligations in this Chapter, as determined by the Authority shall apply only to significant data fiduciaries-

(a) data protection impact assessments under section 33;
(b) record-keeping under section 34;
(c) data audits under section 35; and
(d) data protection officer under section 36.

(4) Notwithstanding sub-section (3), the Authority may notify the application of all or any of the obligations in sub-section (3) to such data fiduciary or class of data fiduciaries, not being a significant data fiduciary, if it is of the view that any processing activity undertaken by such data fiduciary or class of data fiduciaries carries a risk of significant harm to data principals."

III.2 *Analysis*

III.2.1 On review of the draft Sections 29 to 39, it is abundantly clear that some data fiduciaries can be classified as significant data fiduciaries and yet some may be notified by the Authority, in which cases they must comply with any or all obligations under Chapter VII,

specifically, they may be required to comply with requirements of data audits, record keeping, data protection impact assessments and data protection officer => which means that

- Perusal of the language used in Sections 33 (data protection impact assessment), 34 (record keeping), 35 (data audits) and 36 (data protection impact assessments) uses the term "data fiduciaries", instead of significant data fiduciaries or other fiduciaries notified by the Authority under Section 38, creating the impression that all fiduciaries irrespective of their size and scale must comply with the obligations contained in Sections 33, 34, 35, and 36.

- There is inconsistency in drafting if the intent is to limit applicability of the above mentioned 4 sections only to certain classes of fiduciaries.

- While obligation for record keeping under Section 34 must apply to all data principals as explained in subsequent points, obligations of data protection impact assessments, data audits, and data protection officer could be onerous and financially burdensome for medium and small sized entities and accordingly, suitable exceptions should be carved out by limiting applicability of Sections 33, 35 and 36 only to significant or other notified fiduciaries under Section 38.

- Regarding record keeping, all fiduciaries must be required to comply failing which transparency and accountability principles of data processing are nullified, as the data fiduciary cannot account for or provide periodic notice of processing activities to the data principal.

- Further without requiring all data fiduciaries to maintain processing records under Section 34, data principal's right to seek confirmation and access are meaningless.

III.3 *Recommendation*

In light of the analysis above, we recommend that

- Sections 29 (privacy by design), 30 (transparency), 31 (security safeguards), 32 (personal data breach), 34 (record keeping), 37 (processing by entities other than data fiduciaries), and 39 (grievance redressal) are applied to all data fiduciaries, and

- Sections 33 (data protection impact assessment), 35 (data audits), and 36 (data protection officer) should be made applicable to significant and other notified classes of data fiduciaries. Accordingly, it is required that the language is revised suitably in Sections 33, 35 and 36 to bring out the distinction in terms of applicability.

IV. *Obligations and liabilities of processors and sub-processors*

IV.1 Draft section 38 of DPB 2018 deals with processing by entities other than data fiduciaries and states:

"*37. Processing by entities other than data fiduciaries-*

(1) The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.

(2) The data processor referred to in sub-section (1) shall not further engage, appoint, use or involve another data processor in the relevant processing on its behalf except with the authorization of the data fiduciary, unless permitted through the contract referred to in sub-section (1).

(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential."

IV.2 *Analysis*

IV.2.1 Perusal of DPB 2018 and specifically draft Section 37 reveals that all obligations for legal processing are imposed on data fiduciaries, and as long as data processors work within the lawful contract executed with the data fiduciary for the relevant processing activity, they cannot be held liable for any non-compliance or breach of DPB 2018 **=>** which means that

- Data processors are not accountable for compliance with key principles of processing as provided under draft Sections 4 (fair and reasonable processing), 6 (purpose limitation), 7 (collection limitation), 9 (data quality), 10 (data storage limitation), and 11 (accountability).

- Further, they are not legally obligated to adhere to transparency and accountability measures under Chapter VII namely draft Sections 29 (privacy by design), 30 (transparency), 31 (security safeguards), 32 (personal data breach), 34 (record keeping), and 39 (grievance redressal).

- Additionally, they are also not obligated to respect data principal's rights provided under Chapter VI, like draft Sections 24 (right to confirmation and access), 25 (right to correction, etc.), 26 (right to data portability), and 27 (right to be forgotten).

- There is no separate penalty or fine imposed on the data processor for breach of the legal principles and obligations of processing and while the allocation of liability may be contractually determined between the data principal and processor, there will be no deterrent effect on data processors in absence of any penalty or fine.

- Such exclusion of data processors from the above core principles and legal obligations is bound to crumble the data protection regime contemplated under DPB 2018, because in reality, most processing activities stretching through the entire data life cycle (i.e. from collection to destruction) are performed by data processors and as such their

obligations should not be derived from the contract with the data fiduciary, but should be substantiated in law.

- Even though data processing is happening for and on behalf of the data fiduciary, the technical aspects and control over personal data being processed remains with the data processors and hence, it is imperative that data processors are regulated directly under the DPB 2018.

- Furthermore, in absence of any guidance on what are the legal obligations and liabilities of data processors *vis-a-vis* the data fiduciary and data, there is no guidance on how contractual arrangements should operate inter se, which may expose the data processors to unreasonable contractual obligations without limitation of liability where data fiduciary chooses to pass over its compliances under DPB 2018 to the processor in totality. In such situation, the data processor shall similarly expose the sub-processor to processing obligations and liabilities as the fiduciary did to the processor. This will create imbalance of power and affect the contractual freedom available to data processors and sub-processors.

IV.3 *Recommendation*

IV.3.1 To avoid ambiguity with respect to processor obligations and to ensure that the processing principles are followed at every stage of data processing, rights of data principals are safeguarded and unreasonable contractual obligations are not imposed by data fiduciary, the approach followed in Article 28 of EU GDPR may be followed and accordingly, we suggest that Section 37 should be amended in the following manner:

"*37. Processing by entities other than data fiduciaries-*

(1) The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid written contract which shall contain all the relevant details of the processing activities to be performed by the data processor including the types of personal data and sensitive personal data being processed, nature and purpose of processing, and it shall also stipulate that the data processor:

(a) adheres to the principle of fair and reasonable processing under Section 4;
(b) carries out processing activities guided by purpose limitation under Section 5, collection limitation under Section 6 and storage limitation under Section 7;
(c) processes personal data and sensitive personal data only on documented instructions from the data fiduciary;
(d) ensures that persons authorised to carry out such processing activities have committed themselves to confidentiality;
(e) institutes and implements necessary safeguard measures for data security under Section 31;
(f) implements privacy by design under Section 30;
(g) maintains records of processing as required and applicable under Section 34;
(h) reasonably cooperates with the data fiduciary when there is a personal data breach in order to mitigate the risks and harm arising from such breach and notifying the Authority and enabling the data fiduciary to comply with the obligations under Section 32;

(i) engages another data processor as per sub-section 2;
(j) reasonably assists the data fiduciary by instituting appropriate measures for the fulfilment of the data fiduciary's obligation to respond to requests for exercising the data principal's rights laid down in Chapter VI;
(k) reasonably assists, and makes available all information as may be requested by the data fiduciary in ensuring compliance with the provisions of this Act and specifically for enabling the data fiduciary to comply with accountability principle under Section 11 and transparency under Section 30; and
(l) any other requirement as maybe prescribed by the Authority.

(2) Data fiduciary shall only engage data processors who provide sufficient guarantees to implement appropriate security safeguards as per Section 31.

(3) The data processor referred to in sub-section (1) shall not further engage, appoint, use or involve another data processor in the relevant processing on its behalf except with the authorization of the data fiduciary, unless permitted through the contract referred to in sub-section (1).

(4) Where the data processor referred in sub-section (1) engages, appoints, uses or involves another data processor as sub-processor under sub-section (3), the data processor must ensure that the sub-processor is appointed, engaged, used or involved in the relevant processing through a valid written contract and is obligated to comply with the requirements as are made applicable to the data processor under the contract executed between the data processor and the data fiduciary under sub-section (1).

(5) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential."

(6) Where a data processor commits an act or omission in contravention of this Act by determining the purpose and means of processing, the processor shall be considered to be a data fiduciary with respect to that processing activity.

IV.3.2 Additionally, we suggest that statutory liability should be fixed on data processors, including sub-processors for breach of the statutory requirements under DPB 2018, and accordingly we suggest adding the following new Section 73:

"*73. Penalty for data processors in contravention of the Act-*

(1) If any data processor is engaged in processing activities which causes damage, the data processor shall be liable to the extent that it has not complied with obligations of this Act or where it has acted in contravention of lawful instructions of the data fiduciary.
(2) Any data processor held liable under sub-section (1) shall be liable to a penalty subject to a maximum of one crore rupees."

V. ***Obligations and liabilities of joint data fiduciaries***

V.1 The DPB 2018 defines "data processor" under draft Section 3(13) to mean "*any person, including the State, a company, any juristic entity, any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.*" Further, in draft Section 75(5) and in the context of compensation payable to data principal, it is provided that "*where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal as per this section, then each data fiduciary or data processor may be ordered to pay the entire compensation for the harm in order to ensure effective and speedy compensation to the data principal.*" Furthermore, Section 75(6) states that "*where a data fiduciary or data processor, has in accordance with sub-section (5) paid the entire amount of compensation for the harm suffered by the data principal, such data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused.*"

V.2 *Analysis*

V.2.1 On combined reading of Sections 2(13), 75(5) and 75(6), it is evident that DPB 2018 contemplates scenarios where more than one data fiduciary determine the purpose and means of processing **=>** which means that

- All the data fiduciaries involved in the processing activities for same pool of personal data and purpose are obligated to comply with same set of requirements under DB 2018. This could lead to redundancy and repetition; for instance, both data fiduciaries will be maintaining processing records, or both will perform data protection impact assessments.

- There is no guidance on how joint data fiduciaries will inter se allocate obligations and liabilities under contractual arrangement.

- Instances may arise where data fiduciaries may shirk responsibilities or allocate blame on other data fiduciaries, amongst other actions, which will result in the rights of the data principal being impeded or non-compliance with the DPB 2018.

- This can give rise to several disputes where joint data fiduciaries allege and blame the other for the harm caused to the data principal for recovery of compensation paid by one.

V.3 *Recommendations*

The abovementioned issues can be avoided by incorporating specific obligations, which will bring clarity to their functions, streamline various processes, reduce disputes between multiple data fiduciaries, and avoid multiplicity of work, thereby increasing the efficiency of data fiduciaries while complying with the DPB 2018. In order to address this situation, it is worthwhile that DPB 2018 amends Section 12 dealing with accountability in the following manner:

"*12. Accountability*

(1) The data fiduciary shall be responsible for complying with all obligations set out in this Act in respect of any processing undertaken by it or on its behalf.

(2) The data fiduciary should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act.

(3) When two or more data fiduciaries act jointly, they shall determine their respective responsibilities in order to comply with all the obligations set out in this Act by executing a valid written contract, particularly with regard to the exercising of rights of the data principal and the corresponding duty to provide information as provided for in Chapter VI of this Act, including the designation of a point of contact for data principals.

(4) The contract referred in sub-section 12(3) shall duly reflect roles and relationships of the joint data fiduciaries inter se and vis-a-vis the data principals and data processors, and the joint data fiduciaries must acknowledge and agree that the data principal and data processors can exercise their legal or contractual rights against any one the joint data fiduciaries."

****