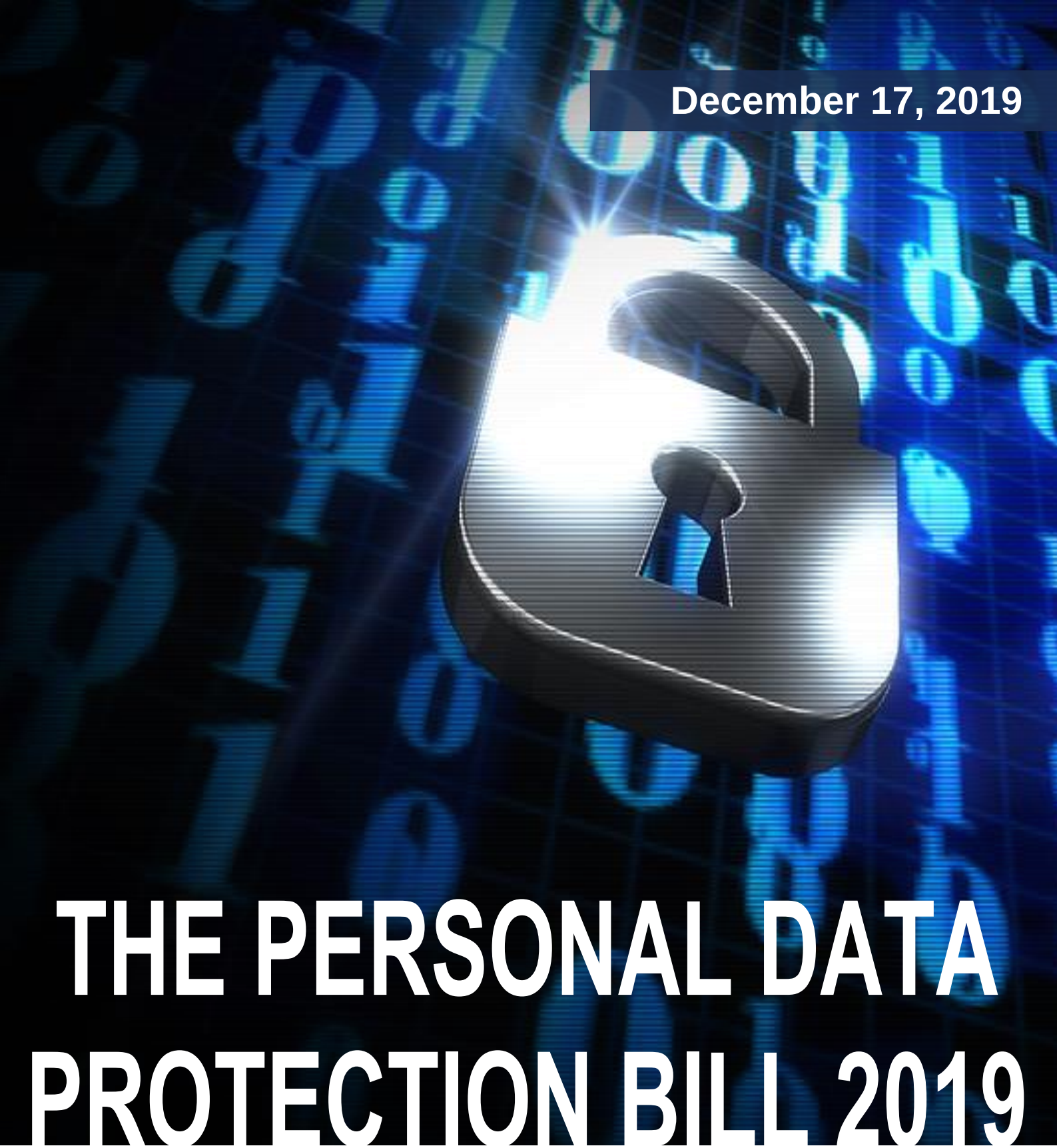

December 17, 2019

THE PERSONAL DATA PROTECTION BILL 2019

- A COMPARISON WITH THE 2018 BILL

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA

Introduction

The latest version of the Personal Data Protection Bill, 2019 ("**2019 Bill**") has been in the public domain since December 10, 2019 and we have compared the latest version against the Personal Data Protection Bill, 2018 ("**2018 Bill**").

Significant Changes

The clauses have been shuffled and a number of drafting changes have been made, making it difficult to cull out the significant changes, such as the following:

1. Status of employees of data fiduciaries: In the 2018 Bill, the definition of "data processor" specifically stated that it did not include an employee of a data fiduciary. The 2019 Bill does not have the same carve-out for employees of data fiduciaries. Does this mean employees of data fiduciaries shall bear the same responsibilities and obligations as data processors? If an employee of a data fiduciary were to be treated as a data processor, such employees would have to implement security safeguards, carry out periodic review of security safeguards etc. Such an interpretation does not seem plausible and hence we assume that this deletion was made because the drafters felt that the carve-out for employees of the data fiduciary is unnecessary. Do please note that both the 2018 Bill and the 2019 Bill state that 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 from such data fiduciary as confidential.

2. Personal data to include inferences drawn: The definition of "personal data" has been modified by the 2019 Bill to provide that "personal data" shall include any inference drawn from such data for the purpose of profiling. Thus, if the personal data available leads to an inference regarding the data principal's gender or age or sexual orientation or income or any other personal attribute of the data principal, such inference shall also be personal data.

3. Omission of "password" from definition of "sensitive personal data": "Password" has been omitted from the list of items that fall within the definition of "sensitive personal data".

4. Withdrawal of Consent - Implications: Both the 2018 Bill and the 2019 Bill allow the data principal to withdraw the consent given to the data fiduciary for processing of his/her personal data. Clause 12(5) of the 2018 Bill provided that "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." The aforementioned language has been modified in the 2019 Bill and Clause 11(6) of the 2019 Bill now states that "where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal." Therefore, if a data principal withdraws his consent for the processing of his/her personal data for a valid reason, such data principal shall not be liable for the legal consequences for the effects of such withdrawal.

5. Omission of "Function of Parliament or any State Legislature" exemption: Clause 13(1) of the 2018 Bill provided that "Personal data may be processed if such processing is necessary for any function of Parliament or any State Legislature." "Function of Parliament or any State Legislature" is a delightfully vague term and this sub-clause has been omitted by the 2019 Bill in the clause setting out grounds under which personal data may be processed without the consent of the data principal. The 2019 Bill continues to provide that personal data may be processed without the consent of the data principal for the

performance of any function of the State which has been authorised by law for (i) the provision of any service or benefit to the data principal from the State; or (ii) the issuance of any certification, licence or permit for any action or activity of the data principal by the State. It may also be processed under any law for the time being in force made by the Parliament or any State Legislature.

6. Processing of personal data in relation to employment: The 2018 Bill allowed personal data, including sensitive personal data, to be processed without the data principal's consent, for purposes related to employment. In the 2019 Bill, only personal data which is not sensitive personal data, can be processed without the data principal's consent, for purposes related to employment.

7. Right to seek erasure: The Right to correction provided for by clause 25 of the 2018 Bill gave a data principal whose personal data is being processed by a data fiduciary, the right to seek correction of inaccurate or misleading personal data, the completion of incomplete personal data and the updating of personal data that is out of date. There was no right to have personal data erased even if such personal is no longer necessary for the purpose for which it was processed. Clause 18(1)(d) of the 2019 Bill provides that a data principal whose data is being processed has the right to seek erasure of his/her personal data which is no longer necessary for the purpose for which it was processed. This right is unconnected with the right to be forgotten which requires a different procedure to be followed for the exercise of that right.

8. Manner of exercise of data principal's rights: In the context of exercise of rights by a data principal, Clause 28(6) of the 2018 Bill provided that the manner of exercise of rights shall be in such form as may be provided by law or in the absence of such law, in a reasonable format to be followed by each data fiduciary. Thus, a data fiduciary could prescribe the manner in which a data principal could exercise his/her rights, if the law did not provide for the same. This provision is missing in the 2019 Bill.

9. Social media intermediaries: The 2019 Bill introduces the concept of a "social media intermediary" and defines the same in the explanation to Clause 26(4). This definition excludes those which primarily enable commercial/ business transactions. The Central Government shall be entitled to notify entities to be social media intermediaries on the basis of the number of users for such intermediaries and their impact on electoral democracy, state security, public order etc. It appears that entities such as Facebook, Snapchat, Twitter etc. would be prime candidates to be social media intermediaries.

   Clauses 28(3) and 28(4) of the 2019 Bill provide that every social media intermediary which is notified as a significant data fiduciary shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed. Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed. We assume that the rules to be framed shall prescribe the manner in which users of social media intermediaries could provide KYC documents to the social media intermediaries and receive visible marks of such verification. Thus, Facebook users could submit KYC documents to Facebook and be identified as genuine users (as opposed to bots) on their Facebook profiles.

   The timely implementation of processes and effective adherence to obligations by social media intermediaries will be subject to an audit by an independent data auditor who audits significant data fiduciaries.

10. Wider construction of "harm" caused from data processing: For the purpose of notifying data fiduciaries or classes of data fiduciaries as significant data fiduciaries, Clause 38(1) of the 2018 Bill had an omnibus sub-clause (f), namely any factor (other than factors

expressly mentioned in Clause 38) which was causing harm to any data principal as a consequence of such processing could be a ground for notifying a data fiduciary as a significant data fiduciary. Under Clause 26(1)(f) of the 2019 Bill, this ground has been amended to read as "any other factor causing harm from such processing". In other words, the harm caused by the data processing need not be suffered by the relevant data principal. It might be suffered by any other person or even the society at large.

11. Storage of personal data: Clause 40(1) of the 2018 Bill required every data fiduciary to ensure that a serving copy of personal data to which the Personal Data Protection Act applies, be stored in India. This requirement applied to all personal data and not only sensitive personal data and the only exemption could be on the grounds of necessity or strategic interests of the State. The 2019 Bill does not have the requirement that at least one serving copy of all Indian personal data be stored in India. It is interesting to note that the 2018 Bill did not define or clarify the meaning of a "serving copy" of personal data.

12. Transfer of critical personal data outside India: Both the 2018 Bill and the 2019 Bill provide that critical personal data cannot be stored outside India, subject to two exceptions. The language of the second exemption differs between the two bills in certain respects. Under the 2018 Bill, the second exemption covers prescribed countries, or prescribed sectors within a country or prescribed international organisations where the Central Government is satisfied that such transfer or class of transfers is necessary for any class of data fiduciaries or data principals and does not hamper the effective enforcement of the Personal Data Protection Act. Under the 2019 Bill, the second exemption covers countries or any entity or class of entity in a country or international organisations, where the Central Government has deemed such transfer to be permissible and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State.

13. Composition of Selection Committee: The 2018 Bill provided that the Data Protection Authority of India ("**DPAI**") shall be appointed by a Selection Committee comprising of (a) the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, who shall be the chairperson of the selection committee, (b) the Cabinet Secretary; and (c) one expert of repute to be nominated by the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, in consultation with the Cabinet Secretary. Under the 2019 Bill, the Selection Committee comprises of (a) the Cabinet Secretary, who shall be Chairperson of the selection committee; (b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and (c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.

14. Additional categories of sensitive personal data: Under the 2018 Bill, the DPAI could specify additional categories of sensitive personal data over and above those listed in the 2018 Bill. This power has now been transferred to the Central Government. Under Clause 15 of the 2019 Bill, the Central Government in consultation with the DPAI and the relevant sectoral regulator shall specify additional categories of sensitive personal data.

15. Prior approval from Central Government for issuance of regulations: Unlike the 2018 Bill, the 2019 Bill has at its end, a brief note on each of its sections after which, there are memoranda on Clause 93 (which deals with the central government's power to make rules) and on Clause 94 (which deals with the DPAI's power to make regulations). The memorandum relating to Clause 94 states that the regulation making powers of the DPAI can be exercised only with the previous approval of the Central Government. The 2018 Bill did not have such memoranda and the DPAI was not required to seek the previous approval of the Central Government before issuing any regulation.

16. DPAI's power to issue guidance: Under the 2018 Bill, the DPAI had the power to issue guidance on any provision under the Personal Data Protection Act, either on its own or in response to any query received from a data fiduciary, if the DPAI considered it necessary to issue such guidance. This power has been taken away in the 2019 Bill.

17. Advisory power of the DPAI: Under the 2018 Bill, the DPAI had the power to advise the Central Government on the acceptance of any relevant international instrument relating to protection of personal data. This power has been taken away in the 2019 Bill. Instead, the 2019 Bill gives the DPAI the power to advise the Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensure consistency of application and enforcement of the Personal Data Protection Act, something which the 2018 Bill failed to do.

18. Searches and seizures: In the context of searches and seizures, the 2018 Bill gave the DPAI (acting through a senior officer) wide ranging powers to carry out searches and seizures. Under the 2019 Bill, the search and seizure powers of the DPAI (to be exercised through Inquiry Officers) appears to be reduced. The power to break open locks, access any computer or seize data etc. which were specifically mentioned in the 2018 Bill, are missing. Further, the 2019 Bill states that Inquiry Officers can only act after obtaining a court order, unlike the 2018 Bill which did not place such a prior restraint.

19. Transfer or selling of personal data: Chapters XIII of the 2018 Bill and the 2019 Bill deal with offences relating to data privacy. Two sections of the 2018 Bill dealing with the offences of knowingly or intentionally or recklessly obtaining or disclosing or transferring or selling personal data or sensitive personal data in contravention of law, have been omitted from the 2019 Bill. It is possible that the drafters wanted to avoid any conflict with the Indian Penal Code, 1860 since these offences can be punished as theft or fraud under the Indian Penal Code, 1860.

20. Transitional provisions: Chapter XIV of the 2018 Bill had a set of transitional provisions which imposed a number of deadlines for implementing the Personal Data Protection Act once it was enacted. The 2019 Bill does not have such a chapter. Therefore, the deadline to set up the DPAI within 15 months of enactment is absent in the 2019 Bill.

21. Central government's power to requisition data for policy formulation: Clause 91(2) of the 2019 Bill gives the Central Government the power to, in consultation with the DPAI, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed. Thus, the Central Government may direct any commercial organisation or even an NGO to hand over its operational data (with the personal data anonymised) to enable the Central Government to make policies. The heading to Clause 91 states that the policies are for "digital economy" and there is a reference to digital economy in Clause 91(1) as well. However, Clause 91(2) does not make any mention of "digital economy" and the data collected under Clause 91(2) could be for the framing of a policy unconnected with the digital economy. Clause 91(3) requires the Central Government to disclose annually the directions, made by it under Clause 91(2).

22. Amendment of RTI Act: The 2018 Bill proposed amendments to the Information Technology Act, 2000 and the Right to Information Act, 2005 ("**RTI Act**"). The former amendments have been retained by the 2019 Bill, whilst the latter (the amendments to the RTI Act) have not. The amendments proposed to the RTI Act by the 2018 Bill provided that personal data need not be disclosed under the RTI Act if such disclosure if likely to cause 'harm' to a data principal, where such 'harm' outweighs the public interest in accessing such information having due regard to the common good of promoting transparency and accountability in the functioning of the public authority. Thus, the proposed amendment to

the RTI Act had substantially widened the scope of the current exemption under Clause 8(1)(j) of the RTI Act and gave more leeway to Information Officers for rejecting a request for disclosure of information and would have curbed the citizens' right to information.

23. State Exemption: Clause 35 of the 2019 Bill has a new provision which states that where the Central Government is satisfied that it is necessary or expedient; (i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.

Other Changes

We found a number of other "not-so-significant" changes, which are:

1. Permissible use of anonymised personal data: Both the 2018 Bill and 2019 Bill state that they do not apply to the processing of anonymised data. However, Clause 91 of the 2019 Bill allows the Central Government, in consultation with the DPAI, direct any data fiduciary or data processor to provide any anonymised personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.

2. Definition of Aadhaar Number deleted: The 2018 Bill defined "Aadhaar Number" and this definition was used in the definition of "Official Identifier", which was an inclusive definition. The 2019 Bill has done away with the definition of "Aadhaar Number" and the definition of "Official Identifier" does not refer to Aadhaar Number, but that doesn't impact the definition of "Official Identifier".

3. "In writing" – New definition: The 2019 Bill has a new definition for "in writing" and it states that "in writing" includes any communication in electronic format as defined in clause (r) of sub-clause (1) of Clause 2 of the Information Technology Act, 2000. This is a case of stating the obvious and is evidently because many of us are yet to recognise electronic format as the same as "in writing" as mandated by the Information Technology Act, 2000. Both the 2018 Bill and 2019 Bill use "in writing" at least 10 times.

4. Steps taken to ensure quality of data: In the context of the data fiduciary's obligation to ensure data quality of personal data stored or processed by such fiduciary, the 2018 Bill required the data fiduciary to take reasonable steps to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed. In the 2019 Bill, the word "reasonable" has been replaced with "necessary". Thus, if a step is necessary, but is not reasonable in the context of effort or cost involved, the data fiduciary must still take such step.

5. The language of the data storage limitation has been tightened: The 2018 Bill stated that: "The data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed."

   The 2019 Bill states that: "The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing."

Further, under the 2018 Bill, personal data could be retained for a longer period if explicitly mandated, or necessary to comply with any obligation, under a law. Under the 2019 Bill, personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force.

6. Operation of search engines added to the list of reasonable purposes: Both the 2018 Bill and the 2019 Bill allow personal data to be processed without the consent of the data principal, if such processing is necessary for such reasonable purposes as may be specified by regulations. However, the 2019 Bill has added the 'operation of search engines' to the list of "reasonable purposes" for which the DPAI may lay down safeguards through regulations.

7. Data Principal's right to access information pertaining to data fiduciaries: Clause 17(3) of the 2019 Bill provides that the data principal shall have the right to access in one place, the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations. This right was not available under the 2018 Bill.

8. Introduction of "consent manager": The concept of "consent manager" has been introduced in the 2019 Bill whereby a data principal can act through a consent manager when exercising his/her rights under the 2019 Bill. Clause 23 of the 2019 Bill defines a "consent manager" for the purpose of Clause 23 of the 2019 Bill, even though the term "consent manager" is also used in Clause 21 of the 2019 Bill. The DPAI has the power to make regulations regarding the manner and the technical, operation, financial and other conditions for registration of the consent manager and its compliance under law.

9. Reasons for rejecting request to exercise any right by the data principal: Where a data principal's request for exercise of any right made to a data fiduciary is rejected by such data fiduciary, the 2018 Bill required the data fiduciary to provide adequate reasons in writing for such rejection. The 2019 Bill has deleted the word "adequate". It is sufficient if the reason for rejection is provided by the data fiduciary.

10. Privacy by design policy: Clause 22 of the 2019 Bill requires every data fiduciary to produce a privacy by design policy. This obligation was present under the 2018 Bill as well. However, the 2019 Bill goes further and puts in place a mechanism for certification of such policy by the DPAI. Clause 22 (2) of the 2019 Bill uses the word 'may' when it states that "subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under sub-clause (1) to the DPAI for certification within such period and in such manner as may be specified by regulations". However, in the given context, one gets the impression that this certification is mandatory. The certified privacy by design policy is required to be published on the website of both the data fiduciary and the DPAI.

11. Conduct of inquiries by Inquiry Officers: Just like the 2018 Bill, the 2019 Bill also provides that when conducting an inquiry into whether the activities of any data fiduciary or data processor are being conducted in a manner which is detrimental to the interest of data principals or if any data fiduciary or data processor has contravened any of the provisions of the Personal Data Protection Act or the rules or regulations made thereunder, or any direction of the DPAI, the DPAI can appoint one of its officers as an Inquiry Officer to inquire into the affairs of such data fiduciary or data processor and to report to the DPAI on any inquiry made. In matters relating to searches and seizures, where the 2018 Bill stated that the DPAI had certain powers, the 2019 Bill states that such powers are with Inquiry Officers. For example, the 2018 Bill stated that the DPAI has the power to call for

information from, conduct inspections and inquiries into the affairs of data fiduciaries. The 2019 Bill states that Inquiry Officers have the aforementioned powers.

12. Qualifications for appointment to the Appellate Tribunal: The 2018 Bill did not spell out the qualifications required to be appointed to the Appellate Tribunal. The 2019 Bill does. The chairperson of the Appellate Tribunal shall be a former Judge of the Supreme Court or a former Chief Justice of a High Court. Other members should have held the post of Secretary to the Government of India or any equivalent post in the Central Government for a period of not less than two years or a person who is well versed in the field of data protection, information technology, data management, data science, data security, cyber and internet laws or any related subject.

13. Cognizance of offences: The 2019 Bill states in Clause 83(2) that no court shall take cognizance of any offence under the Personal Data Protection Act, unless a complaint is made by the DPAI.

14. Introduction of a regulatory sandbox: A regulatory sandbox is a controlled environment created by a regulator to allow live testing of new products or services aided by exemptions from certain regulations. Clause 40 of the 2019 Bill requires the DPAI to create such a sandbox for the purpose of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest.

15. Exemptions extended to small entities: Data fiduciaries which fall below certain criteria are classified as 'small entities' by the 2018 Bill and these small entities are eligible for certain exemptions from the obligations applicable to data fiduciaries. The specified criteria were turnover not exceeding twenty lakh rupees, not collecting personal data for the purpose of disclosure to any other individuals or entities, including other data fiduciaries or processors and not processing personal data of more than one hundred data principals in any one day in the preceding twelve calendar months. The 2019 Bill has removed the aforementioned quantifications and the DPAI has been given the responsibility of framing regulations setting out such quantifications.

16. Extent of the enactment: The 2018 Bill specifically stated (in Clause 1(2)) that it extends to the whole of India, but the 2019 Bill does not have an equivalent provision. This could be because both the 2018 Bill and the 2019 Bill state that they apply to the processing of personal data by data fiduciaries or data processors outside India, if such processing is in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India or in connection with any activity which involves profiling of data principals within the territory of India.

17. Processing of data with the consent of the data principal: The 2018 Bill provided that processing of personal data could be undertaken with the consent of the data principal. There were also other grounds for processing personal data. The 2019 Bill states that personal data can be processed only with the consent of the data principal, subject to a number of exceptions. The net effect is that the importance of consent is brought into sharper focus, but there is no substantial change.

18. Right to be Forgotten: In the context of the Right to be Forgotten, the 2019 Bill has inserted a new sub-clause (5) in Clause 20 to state that any person aggrieved by an order made under Clause 20 by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal. Clause 39(5) of the 2018 Bill had provided a general right of appeal against orders passed by Adjudicating Officers which gave the impression that it did not specifically apply to orders passed in connection with the Right to be Forgotten under Clause 27.

19. Processing of personal data: Clause 37(3) of the 2018 Bill provided that 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. Clause 31(3) of the 2019 Bill deals with the same topic, but has done away with words “unless they are required to do otherwise under law” as a result of which the data processor, employees of the data fiduciary or the data processor merely have to process personal data in accordance with the instructions of the data fiduciary. They do not have the option to act otherwise, even if they are of the view that the data fiduciary’s instructions are contrary to law.

20. “Shall” instead of “must”: And finally, we note that in a number of places, “must” has been replaced by the word “shall”. Generally, statutes and legal documents, prefer the word “shall” over words like “must” or “will’.

This update has been contributed by Vinod Joseph (Partner) and Protiti Basu (Associate).

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com