KHAITAN &CO
Advocates since 1911

NEWSFLASH

ERGO
Analysing developments impacting business

DECODING THE PERSONAL DATA PROTECTION BILL, 2018

9 August 2018

Genesis of the Draft Bill and the Way Forward

In July 2017, the Ministry of Electronics and Information Technology, Government of India had constituted a committee of experts (Committee) under the chairmanship of a retired judge of the Supreme Court, Mr B N Srikrishna, to examine and propose changes to the data protection regime in India. In December 2017, the Committee published a white paper on the data protection framework proposed for India and invited public comments on the same. The Personal Data Protection Bill, 2018 (Draft Bill) has now been proposed after discussions and deliberations by the Committee, both internally as well as with various stakeholders.

The Draft Bill is largely inspired by the European Union's General Data Protection Regulation, which became effective from 25 May 2018 (GDPR). The Draft Bill provides for a phase wise implementation of its provisions over 18 months upon enactment.

➢ Key Definitions under the Draft Bill

Data Fiduciary	•Any person (including the State, a company, any juristic entity or any individual) who determines the purpose and means of processing of personal data.
Data Processor	Any person (including the State, a company, any juristic entity or any individual) who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.
Data Principal	A natural person to whom the personal data relates.
Personal Data	Data about a natural person in relation to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.
Sensitive Personal Data	Personal data revealing, related to, or constituting passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious political belief or affiliation, or any other catgory as may be specified by the Data Protection Authority of India (Authority).

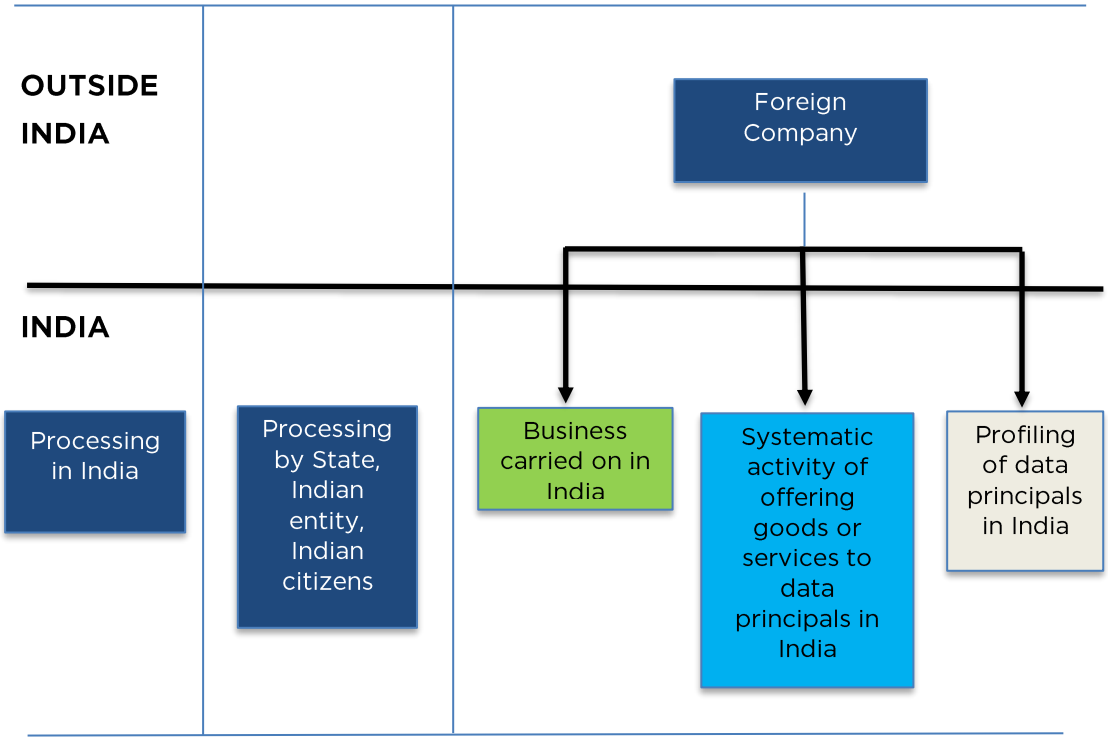
Comment

The definition of 'sensitive personal data' has been significantly broadened as compared to the present definition of the term under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. In fact, it is wider than the ambit of sensitive personal data under GDPR. Therefore, organisations processing sensitive personal data will be subject to additional compliance requirements once the Draft Bill is enacted.

➢ **Applicability of the Draft Bill**

The Draft Bill is intended to apply to processing of personal data within the territory of India by Indian data fiduciaries and data processors. Further, the Draft Bill is also intended to apply to foreign data fiduciaries and data processors, where personal data is processed by them in connection with:

- any business carried on in India; or
- for systematic activity of offering goods or services to data principals within the territory of India; or
- any activity which involves profiling of data principals within India.



Exemptions: The Draft Bill does not apply to anonymised data.

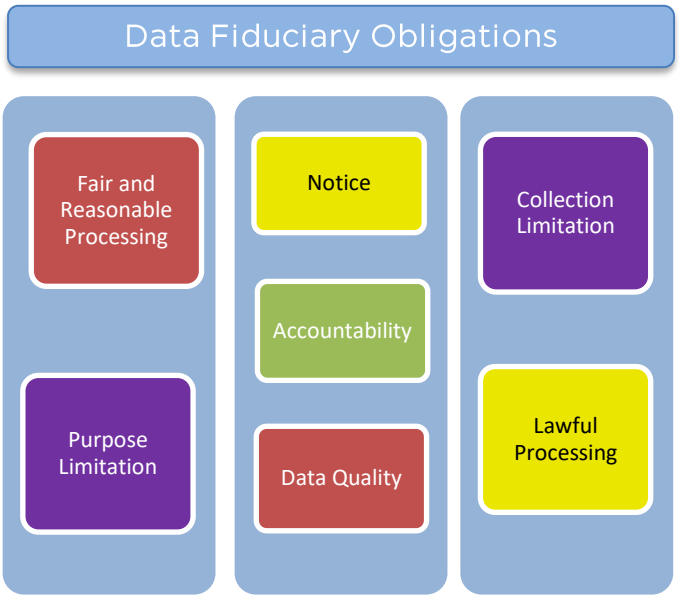
Comment

The Draft Bill has an extra-territorial application and will therefore impose additional compliance requirements for foreign data fiduciaries and data processors. The term "business carried in India" has not been defined, and clarity is needed on this aspect before the Draft Bill is finally enacted. As it currently stands, the Draft Bill may even be applicable to foreign data fiduciaries and data processors who have insignificant commercial relationships in India.

The term, 'profiling', has been defined to mean processing of personal data for analysing or predicting aspects concerning the behaviour, attributes or interest

of a data principal. Therefore, use of online tracking through cookies, etc., would also come under the ambit of the Draft Bill.

➢ **Data Protection Obligations**



The Draft Bill provides for certain principles based on which personal data should be processed. Briefly, the principles are as follows:

- Fair and reasonable processing: A data fiduciary should process personal data in a fair and reasonable manner that respects the privacy of the data principal.

- Collection and purpose limitation: The collection of personal data should be necessary for the purposes of processing. Processing should only be for purposes that are clear, specific and lawful.

- Grounds for processing Personal Data:

Personal data may be processed only on certain grounds, such as:

- Free, informed, specific, clear consent of the data principal is obtained and it is capable of being withdrawn;
- Compliance with law or order of a court or tribunal;
- Prompt action, in case of medical emergency, breakdown of public order, etc.; or
- Employment, recruitment, termination of employment, verifying attendance, assessment of employee, etc.

Additional requirements have been provided in relation to the grounds for processing sensitive personal data.

- Notice: A data fiduciary is required to provide a clear notice to data principal at the time of collection of personal data. Such a notice should, *inter alia,* specify the purpose of processing, categories of personal data being collected, rights of data principals over their personal data, duration of retention, cross-border transfer of data, right to withdraw consent, etc. Such information needs to be provided such that it is easily comprehensible and in multiple languages, where necessary and practicable.

- Personal Data Quality and Storage Limitation: The data fiduciary is required to take reasonable steps to ensure that the personal data processed is complete, accurate, not misleading and updated. The data fiduciary may retain personal data only as long as may be reasonably necessary to satisfy the purpose of processing and may retain it longer only if such retention is explicitly mandated or required to be retained by law.

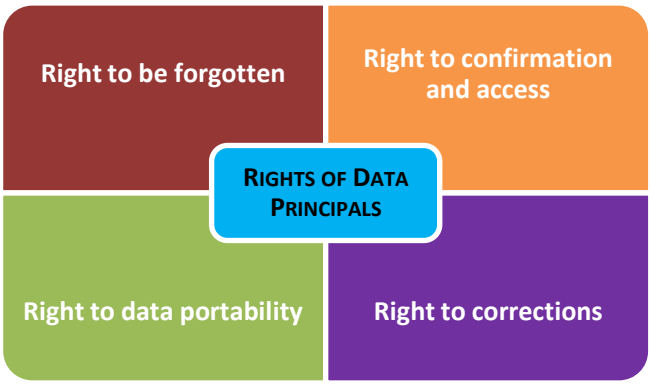
- Accountability: The data fiduciary is responsible for complying with all obligations set out in the Draft Bill and should be able to demonstrate such compliance.

- Exemptions: Certain exemptions have been provided in the Draft Bill in relation to processing of personal data for prevention, detection, investigation and prosecution of contravention of law, security of the State, legal proceedings, research, archiving or statistical purposes, personal or domestic purposes and journalistic purposes.

Comment

The Draft Bill focusses largely on compliances and once this law is enacted, in its current form, it may prove to be cumbersome for data fiduciaries. Further, certain obligations such as the requirement of giving notice, obtaining consent, etc., may pose practical and logistical issues for organisations and compliance with the same would mean additional administrative burden and costs. Providing consent in multiple languages may prove to be a major practical challenge for social media platforms, e-commerce companies, etc., which have a wide base of users across locations.

➢ **Rights of Data Principals**



A data principal has the following rights under the Draft Bill:

- Right to Confirmation and Access: A data principal has the right to obtain confirmation on whether personal data is being processed, a summary of the personal data being processed and a summary of the processing activities.

- Right to Correction: In certain situations where necessary in relation to the purposes for which personal data is being processed, the data principal has the right to request the data fiduciary to correct, complete or update the personal data.

- Right to Data Portability: Subject to certain exceptions, the data principal has the right to receive personal data which has been provided to a data fiduciary in a structured and machine-readable format as well as request the data fiduciary to transfer such personal data to another data fiduciary in the same format.

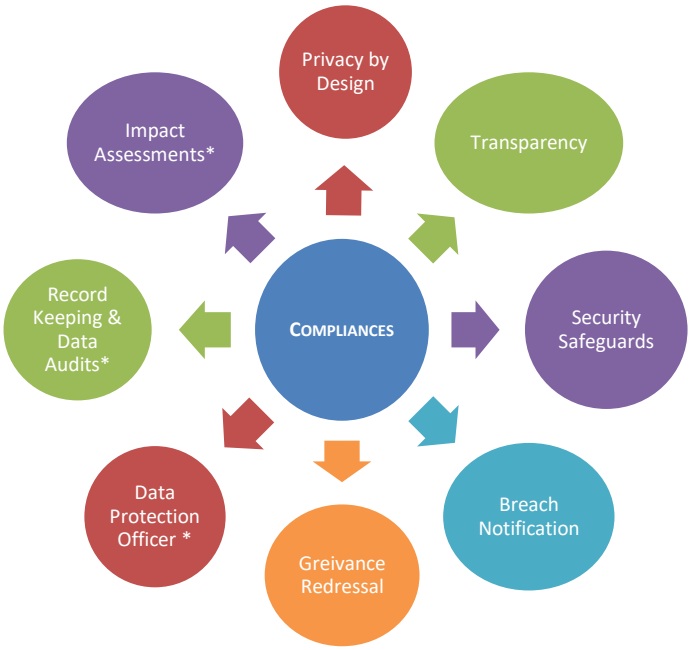
- Right to be Forgotten: The data principal has the right to restrict or prevent the continuing disclosure of personal data in certain situations, such as where the data principal has withdrawn consent, or if the purpose for the same is served.

- Special safeguards for processing personal data of children: Enhanced safeguards have been included for the processing of personal data and sensitive personal data of children (i.e. persons below 18 years of age). A data fiduciary will need to incorporate an appropriate age verification mechanism and obtain parental consent for processing personal data of children.

Comment

The age requirement of 18 years for children is higher than that provided in other jurisdictions. For example, the corresponding age under the GDPR is 16 years and member states in the European Union may specify an even lower age, not below 13 years. The proposed new provisions for processing personal data of children may significantly impact entities targeting children (e.g. online retailers selling toys, subscription boxes, gaming etc.) as well as schools, colleges and universities. Further, organisations will need to enable adequate IT systems to implement the right to be forgotten, right to data portability, etc., which would mean additional cost and time.

➢ **Compliances and Measures to be taken by Organisations**



* *Applicable only to data fiduciaries which may be notified as Significant Data Fiduciaries (SDF), by the Authority based on volume of personal data processed by it, sensitivity of the personal data, turnover of the data fiduciary, risk of harm, use of new technologies, etc. The Authority may also specify certain categories of data fiduciaries, who may not be SDFs, but should comply with these security measures.*

The key compliances and security measures proposed by the Draft Bill include:

Localisation of Personal Data	Data fiduciaries are required to ensure that at least one serving copy of personal data is stored on a server or data centre located in India. Additionally, personal data which is notified as 'critical' by the Central Government are required to be mandatorily processed in a server or data centre located in India.
Privacy by Design	Data fiduciaries are required to implement policies and measures to ensure that the managerial, organisational, technical, technological and business practices of an organisation are designed in a manner to anticipate, identify and avoid harm to a data principal and the interest of the data principal is accounted for at every stage of processing of personal data.
Transparency	Data fiduciaries are required to take reasonable steps to maintain transparency in general practices related to processing of personal data.
Security Safeguards	Data fiduciaries and data processors are required to implement and periodically review appropriate security safeguards considering the nature, scope and purpose of processing of personal data. Some of the measures prescribed include de-identification and encryption of personal data.

Personal Data Breach Notification	▪ Data fiduciaries are required to notify the Authority where breach of personal data is likely to cause harm to a data principal. ▪ The Authority's powers are threefold in this regard: firstly, it has the power to determine whether the data principal should be informed of such breach basis the severity of the likely harm; secondly, it may direct the data fiduciary to take remedial measures; and finally, it can direct the data fiduciary to post details of the data breach and remedial measures taken for the same on its website, and/or do so on the Authority's own website.
Data Protection Impact Assessment	▪ Prior to the introduction of any processing that involves new technologies or large-scale profiling or use of sensitive personal data such biometric data, genetic data, etc. or any other process which carry a risk of significant harm to data principals, a SDF are required to undertake a data protection impact assessment (DPIA) in accordance with the provisions of the Draft Bill. ▪ The Authority may also specify circumstances or classes of data fiduciaries or processing operations where a DPIA shall be mandatory.
Records	A SDF is obligated to maintain accurate and updated records of important operations in the life-cycle of the data, DPIAs, periodic reviews of security safeguards and other information as may be specified by the Authority.
Registration with the Authority	A SDF is required to be registered with the Authority in a manner as may be specified.
Requirement to Conduct Annual Data Audits	A SDF is required to procure that an annual data audit on its policies and processing of personal data is conducted by an independent data auditor on matters which include, *inter alia*, clarity and effectiveness of notices, transparency in processing of personal data and instances of personal data breach.
Appointment of a Data Protection Officer	A SDF is required to appoint a Data Protection Officer (DPO) to carry out specified functions which include advising the data fiduciary on fulfilling its obligations, conducting DPIAs and formulating policies.
Data Processing Agreements	A data fiduciary may engage a data processor only *via* a valid contract. A data processor and its employees are required to be bound by the instructions of the data fiduciary when processing personal data and must treat all personal data received from a data fiduciary as confidential.
Grievance Redressal Mechanism	▪ The data fiduciary is required to establish effective procedures and mechanisms to address grievances of data principals and resolve the same in not more than 30 days.

	▪ A data principal has the right to file a complaint with the Authority if a grievance remains unresolved within the statutory time period or when it is dissatisfied with the manner of resolving the grievance or if the grievance raised has been rejected.

Comment

Data localisation requirements would entail additional time and cost for setting up/ leasing local servers in India, which may especially be a pain-point for start-ups. This would have to be complied with even when an organisation does not have a presence in India but where the provisions of the Draft Bill are applicable to such foreign entities (which do not have a physical presence in India). With the exception of certain exempted categories of processing under the Draft Bill, all entities irrespective of size or scale of processing, would still need to comply with measures such as privacy by design, security standards – encryption and de-identification, breach notifications and transparency obligations.

➢ **Cross-border Data Transfers from India**

Personal data, other than personal data which may be notified by the central government as critical personal data, can be transferred outside India, in certain instances, such as:

- transfer is made subject to execution of standard contractual clauses or intra-group schemes approved by the Authority and notification to the Authority by the data fiduciary;
- where the Central Government in consultation with the Authority, has prescribed that transfer of personal data is permissible to a country, or to a sector within a country or to international organisations; and
- in case only consent is relied upon for transfer of personal data, it should be subject to standard contractual clauses/ intra-group schemes/ transfer to a country that is green lit as having adequate status by the Authority. The Authority may also approve transfer due to a situation of necessity.

	Personal Data	Sensitive Personal Data
CONDITIONS	(a) DPA approved Standard Contractual Clauses / Intra-Group Schemes	
	OR	
	(b) Prescription by Central Government after consultation with DPA	
	OR	
	Consent of Data Principal + (a) or (b)	Explicit Consent of Data Principal + (a) or (b)
	OR	
	DPA approves transfer due to situation of necessity	

Comment

Amongst the various conditions for cross border transfer of personal data, looking at EU experience, it seems that mostly personal data will be transferred under standard contractual clauses. Since even EU has recognized only 12 countries to have adequacy status, the effectiveness of this method is expected to be very limited. Also, there are very few countries in the world that have a robust data protection regime. However, since the adequacy status can also be given to a sector in a country or an international organization under the Draft Bill, the effectiveness of this method will also depend on the proactiveness of the Government.

- **Data Protection Authority and Enforcement Mechanism**

The Draft Bill proposes to establish the Authority, as the nodal agency for its implementation. The Authority will act to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with provisions of the Draft Bill, issue codes of practice for compliance, promote awareness on data protection, call for information and initiate inquiries. For imposing penalties or awarding compensation, the Authority is proposed to have a separate wing and an adjudicating officer is proposed to be appointed to carry out the adjudication related functions.

Comment

The powers granted to the Authority appear to be very wide and discretionary. The Authority has is proposed to function as a supervisory body, enforcement agency and an adjudicatory body. Significantly, the Authority has extensive powers including the power to suspend the business or activity of a data fiduciary or a data processor which is in breach of the provisions of the Draft Bill, conducting search and seizures or suspending or discontinuing cross border flow of personal data.

- **Penalties and Compensation**

The important penalty provisions in the Draft Bill have been divided into two major categories:

- if a data fiduciary does not comply with significant obligations such as contravention of provisions related to sensitive personal data, personal data pertaining to children, cross border transfer of personal data, etc., it shall be liable to a penalty which may extend to INR 150,000,000 (approx. USD 2,200,000) or 4% of its total worldwide turnover of the preceding financial year, whichever is higher; and

- if a data fiduciary does not adhere to certain compliance related requirements such as conducting a DPIA, appointment of DPO, conducting a data audit, obligation to take prompt and appropriate action in response to a personal data breach, etc., it shall be liable to a penalty which may extend to INR 50,000,000 (approx. USD 730,000) or 2% of its total worldwide turnover of the preceding financial year, whichever is higher.

The term total worldwide turnover has been defined to mean the gross amount of revenue in the profit and loss account or equivalent statement (as applicable), and includes revenues generated both within and outside India.

In addition, the Draft Bill prescribes various other graded penalties for both a data fiduciary and a data processor. Data principals may additionally claim for compensation for any harm caused due to contravention of any of the provisions by a data fiduciary or a data processor. Criminal and non-bailable

sanctions have also been proposed for offences such as knowingly or intentionally or recklessly obtaining, transferring or selling of personal data, etc.

Comment

The penalties prescribed under the Draft Bill are quite stringent. Further, compensation can be sought by a data principal against a data fiduciary and/or a data processor, which will be over and above any penalties imposed.

➢ Concluding Remarks

The Draft Bill is quite heavy on compliance and proposes a stringent penalty scheme to act as a deterrent for non-compliance. To balance this approach with economic and trade interests, the Government of India must also be mindful that the final law should meet the adequacy standards as prescribed by similar legislations of other countries, to enable mutual cross border transfer of data.

It is also likely that the Supreme Court judgement in the Aadhaar Case could have some impact on the final form of the Draft Bill.

Considering that certain provisions of the Draft Bill will only take effect after a period of time, it will allow data fiduciaries to prepare their systems and processes to ensure compliance. The Draft Bill is the most prominent step towards a comprehensive law on personal data protection in India. However, some elements in the Draft Bill should ideally be further clarified and discussed with various stakeholders for effective implementation, as discussed in various sections of this newsflash.

We had recently hosted a webinar on this topic. A recording of the same is accessible on link

- *Data Privacy Group at Khaitan & Co*

For any queries please contact: editors@khaitanco.com

Mumbai
One Indiabulls Centre, 13th Floor
Tower 1 841, Senapati Bapat Marg
Mumbai 400 013, India

T: +91 22 6636 5000
E: mumbai@khaitanco.com

New Delhi
Ashoka Estate, 12th Floor
24 Barakhamba Road
New Delhi 110 001, India

T: +91 11 4151 5454
E: delhi@khaitanco.com

Bengaluru
Simal, 2nd Floor
7/1, Ulsoor Road
Bengaluru 560 042, India

T: +91 80 4339 7000
E: bengaluru@khaitanco.com

Kolkata
Emerald House
1 B Old Post Office Street
Kolkata 700 001, India

T: +91 33 2248 7000
E: kolkata@khaitanco.com