AMERICAN CHAMBER OF COMMERCE IN INDIA
PHD House, 4th Floor, 4/2, Siri Institutional Area, August Kranti Marg
New Delhi - 110016 Tel : 91-11-26525201/02, Fax : 91-11-26525203
Email : amcham@amchamindia.com Website : www.amchamindia.com

10th October 2018

Revised Submission of industry viewpoints on Personal Data Protection Bill 2018

Greetings from the American Chamber of Commerce in India (AMCHAM), the apex chamber of U.S. Companies in India. AMCHAM is affiliated to the U.S. Chamber of Commerce, Washington, D.C. Established in 1992, AMCHAM has around 450 U.S. companies as members. Headquartered in New Delhi, the chamber has regional offices in Bengaluru, Hyderabad, Mumbai, Chennai and Kolkata.

AMCHAM would like to submit its view point on Draft Personal Data Protection Bill 2018 based on the inputs received from its members. Our recommendations cover the following chapters from the Personal Data Protection Bill, 2018:

- Chapter 1: Preliminary- [Section 3]
- Chapter 2: Data Protection Obligations- [Section 8, 10]
- Chapter 3: Ground of Processing of Personal Data- [Section 12, 14, 17]
- Chapter 4: Ground for Processing of Sensitive Personal Data- [Section 22]
- Chapter 5: Personal and Sensitive Personal Data of Children- [Section 23]
- Chapter 6: Data Principal Rights- [Section 28]
- Chapter 7: Transparency and Accountability Measure- [Section 29, 31, 32, 33, 34, 35, 36 38]
- Chapter 8: Transfer of Personal Data Outside India- [Section 40, 41]
- Chapter 9: Exemptions [Section 45]
- Chapter 10: Data Protection Authority of India- [Section 62, 63, 64, 65, 66, 75]
- Chapter 11: Penalties and Remedies- [Section 69]
- Chapter 13: Offences- [Section 90, 95]

Our submission is aimed to provide recommendations to make regulatory regime for data protection more effective while ensuring it does not impact the adoption of evolving technologies and business models. We hope these will merit your kind consideration.

CHAPTER 1

Reference: Personal Data Protection Bill, 2018 (Chapter 1: Preliminary [Section 3])

Issues:

Anonymization

Section 3(3) defines anonymization as the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified. The standard of irreversibility is excessive and blind to technological realities, as it is an impracticable standard.

Biometric Data

Section 3(8) defines biometric data in an overbroad manner that renders any data collected by observing individuals as biometric and therefore sensitive personal data. Further, the definition as it stands includes photographs containing facial images, thereby severely restricting common and non-sensitive processing of photographs.

Recommendations

The definition of anonymization should be rationalized, with industry being allowed to come up with their own standards and best practices instead of a prescriptive level of anonymization being mandated by the DPA.

The definition of biometric data should be limited to data which is used for the purpose of confirming the unique identification of a natural person. An explicit exclusion of photographs also needs to be made.

CHAPTER 2

Reference: Personal Data Protection Bill, 2018 (Chapter 2: Data Protection Obligations [Section 8])

Issues:

Notices

Section 8(1): Data Fiduciary shall provide explicit notice to data principal in case of processing of their personal data. However, one of the criteria under point (n) 'any other information as may be specified by the Authority' creates uncertainty for the organizations in terms of content of the privacy notices, which might be required to be changed basis varying specifications provided by the Authority. Further, inclusion of the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, would require change to the notice, whenever the data processor change.

Section 8(2): The Bill requires data fiduciary to provide notice to data principal in multiple languages, where necessary and practicable. However, factor or criteria to determine the applicability of this requirement to data fiduciary is not specified in the Bill.

Recommendations

In most of the organizations, "notice" is global and changes to the same involve a complex process. It would be helpful if the Notice is limited to the purpose with which the information is being collected and will be processed. Any change to the same should be notified to the data principal. However, it may be extremely difficult to institutionalize a process where any change in the operational details of processing of data is required to be communicated to and consented with data principals.

It is recommended that the changes/ updates to the notices are minimized and any open statements must be removed from the Bill or more clear specifications included. For instance, notice should include categories of data fiduciaries or processor with whom the personal data is shared, instead of the individuals or entity names.

The clause should either be deleted from the Bill, or public notification to data principal of any changes to the notice should suffice for this provision.

Reference: Personal Data Protection Bill, 2018 (Chapter 2: Data Protection Obligations [Section 10])

Issues:

Data Storage Limitation

Section 10 of the Draft Bill prohibits data fiduciaries from retaining personal data beyond the period of necessity for satisfying the purpose for which such data was processed. This restricts the ability of data fiduciaries to undertake various analytics and other processes on the data which allows them to enhance their services.

Recommendations

Data fiduciaries should be allowed to retain personal data beyond the period of necessity as long as such data is in a de-identified form. This allows for a balance to be struck between the protection of data principals and the need for businesses to use aggregated data to improve their services.

CHAPTER 3

Reference: Personal Data Protection Bill, 2018 (Chapter 3: Ground of Processing of Personal Data [Section 12, 14, 17])

Issues:

i. Misuse of contract as ground for processing of personal data

As per Justice SriKrishna Committee report, there is a distinction between contract and consent, and reasons that a ground relying on contractual necessity can be easily misused by inserting unrelated data processing activities in the contract and personal data henceforth collected would be deemed to be necessary for such processing activities.

ii. Applicability of consent for processing data collected in the past

Section 12(1) – This clause speaks about the consent to be obtained for processing the data collected by the data fiduciary. The requirement of consent under this clause may be restricted to new data collected under Section 8 of the Bill. The clause in its current form does not differentiate data collected in the past and the data collected post enactment of Section 8.

iii. Processing based on mandate under any law

Section 14(a) – Financial services industry believes that in certain circumstances, regulators like RBI, SEBI, IRDA and UIDAI issue rules/regulations (for instance, additional KYC information), which need to be followed by the market intermediaries. These may not form part of the law made by the Parliament or any State Legislature. Also, consent should not be the ground for such processing. However, the Bill does not provide any provision for such processing.

iv. Processing of personal data necessary for purposes related to employment

Section 16: It includes processing of personal data for the purpose of employment. However, it does not include the following aspects:

Issues such as workplace monitoring through use of CCTV, electronic communication monitoring, new technologies such as DLP, logs etc. are not specifically mentioned or addressed. In absence of any mention of specific labor law requirements, it is not clear if such activities may be carried out based on legitimate interest ground or based on consent and if employees may object to such monitoring.

v. "Reasonable purpose" ground for processing personal data

a. Section 17 - The provision for processing of data for reasonable purposes has a very wide scope, which would give rise to ambiguity and violation of data principal rights owing to lack of clear guidelines.
b. Further, such reasonable purposes ground for processing would be limited to specific purposes to be identified by the Data Protection Authority, rather than analysis of data fiduciary.

Recommendations

i. **Misuse of contract as ground for processing of personal data**

a. Performance of contract should be retained as grounds for processing of personal data. However, suggested approach may be adopted to address the concern related to misuse - Read the provision on purpose limitation in conjunction with the subject matter of the contract, i.e. processing activities under the clauses in a contract must have a strong nexus with the subject matter of the contract.

ii. **"Reasonable purpose" ground for processing personal data**

a. Specific guidelines should be developed to define what should be considered as "interest of the data fiduciary" and "any public interest", and the nexus between the public interest or interest of data fiduciary and purpose of processing to curb future litigation.
Organization have suggested two approaches:

b. Bill should provide provision for "reasonable purpose" to be demonstrated by data fiduciary through a rigorous, documented analysis of privacy risks and mitigation to confirm lawful benefit that fiduciary or third party derive.

c. Data Protection Authority should develop "reasonable purposes" through sufficient industry and public consultation, and further be extended to processing of specific types of sensitive personal data.

iii. **Applicability of consent for processing data collected in the past**

a. The clause 12(1) should be made applicable only to data collected after the enactment of clause 8 related to notice.

b. Since, it is practically not possible to obtain consent of all existing customers, any person who has an objection in processing the existing data may be allowed to raise the same with respective data fiduciary and data processor. If the data fiduciary or data processor has objection to accede to such request, the matter may be referred to the adjudicating authority.

iv. **Processing of personal data necessary for purposes related to employment**

a. Workplace monitoring aspect shall be addressed within the Act to provide overall direction as to till what extent and on what basis such activities might be permissible.

CHAPTER 4

Reference: Personal Data Protection Bill, 2018 (Chapter 4: Ground for Processing of Sensitive Personal Data [Section 22])

Issues:

Grounds for processing of Sensitive Personal Data

Section 22(1): The Bill mentions that Authority may specify additional categories of personal data which shall be sensitive personal data, and any further grounds on which such specified categories of personal data may be processed. AMCHAM believes that having the Authority designate anything as sensitive personal data, and the fact that grounds for processing such data may vary with time, would create uncertainty for the processing of data, and lead to instability in the business processes. Also,

password is included in the definition of Sensitive Personal Data, which means that consent would be required for creation and use of the same.

Section 22(3): The Authority may also specify categories of personal data which require additional safeguards or restrictions (as specified by the Authority) where repeated, continuous or systematic collection for the purposes of profiling takes place. This again creates uncertainty for processing of data and leads to instability in the business processes.

Further, processing of sensitive personal data for purposes related to employment is not a valid ground in the draft Bill, and this needs to be provided for. Passwords, Health data and financials are data defined as sensitive personal data. They are also necessarily processed for by employer to offer various services to employees, and this should be termed a valid ground in the draft Bill.

Recommendations

Categories of sensitive personal data should be clearly defined in the Bill and not subject to additional definitions by the Authority. Passwords and financial information should be removed from definition of sensitive personal data.

Further, the grounds for processing of sensitive personal data, categories of personal data specified in section 22(3) and associated safeguards or restrictions should be clearly defined in the Bill, and not subject to constant change by the Authority.

Processing for the purpose of employment should be a valid ground.

CHAPTER 5

Reference: Personal Data Protection Bill, 2018 (Chapter 5: Personal and Sensitive Personal Data of Children [Section 23])

Issues:

Children Data

Section 23: It imposes additional obligations on data fiduciaries dealing with the personal data of children, i.e. those under the **age of 18**. DPA can notify certain fiduciaries as guardian data fiduciaries if they operate online services directed at children or process large volumes of personal data of children.

Recommendations

a. By defining children as all individuals below the age of 18, the bill overextends the protection for children.
b. It is required to reduce the scope of the definition of children to bring it on parity with international standards.

c. A self-identification mechanism should be sufficient which is the ideal mechanism for age verification. Moreover, technical solutions should be preferred and industry should be encouraged to come up with these through multi-stakeholder initiatives.

Reference: Personal Data Protection Bill, 2018 (Chapter 6: Data Principal Rights [Section 28])

Issues:

Data Principal Rights

Section 28 requires data principal to raise a request in writing, and for data fiduciary to respond in writing (in case of refusal of request).

Recommendations

a. The requestor should be able to request for the personal data in the same manner in which it was provided (for instance, web form). This should preclude self-service modules for data correction.
b. Similarly, electronic notifications or responses should be allowed for data fiduciary.

CHAPTER 7

Reference: Personal Data Protection Bill, 2018 (Chapter 7: Transparency and Accountability Measure [Section 29, 30])

Issues:

Privacy by Design

Section 29(c): Every data fiduciary shall implement policies and measures to ensure that technology used in the processing of personal data is in accordance with commercially accepted or certified standards. However, organizations are of the view that this will impact the ability of the companies to innovate.

Transparency

Section 30(2) imposes an obligation upon data fiduciaries to notify data principals of 'important operations' in the processing of personal data related to the principal through 'periodic' notifications. The terms 'important operation' and 'periodic' are both vague and do not offer any clarity for compliance. These must be clarified.

Recommendations

The IT/ITeS sector is of the opinion that as long as the data protection principles are followed, the use of specific technology should not impact the rights and freedoms of data principal.

Moreover, it is vital to clarify the meaning of 'important operations' and 'periodic' in order for meaningful compliance.

Reference: Personal Data Protection Bill, 2018 (Chapter 7: Transparency and Accountability Measure [Section 31])

Issues:

Responsibility and joint liability

Section 31 imposes responsibility for implementation of security safeguards on both data fiduciary and data processor. However, data processors are of the view that requisite security safeguards to be adopted by data processor should be specified in the contract, as the data fiduciary will have full understanding of the data collected, its purpose and likely harm it can cause. This will also help data fiduciary and data processors to remove any ambiguity that may arise.

For disclosures made to regulators, data fiduciaries will not have any formal contracts with them w.r.t data privacy and security. For example, disclosures made to KRA, CERSAI in the financial sector. It is important therefore that such regulators have appropriate security standards and practices and any data breach or misuse will not make the regulated entity liable.

Recommendations

Primary responsibility for identification of the necessary security standards and safeguards necessary to comply with under the law should be on the Data fiduciary, and they should be specified in the contracts with the data processor, to remove any ambiguity. This is also aligned with the draft Bill provision in Section 37, where data fiduciary can engage data processor through mandatory valid contract to process data on its behalf.

The periodicity for review of security safeguards should be clearly described in the law or be acceptable based on internationally recognized standards.

Reference: Personal Data Protection Bill, 2018 (Chapter 7: Transparency and Accountability Measure [Section 32])

Issues:

Personal Data Breach

Section 32: The Bill elaborates on the following requirements for personal data breach to the Authority and data principal (if required):

a. Sub-section (3): Timelines for personal data breach notification
b. Sub-section (5): Reporting of personal data breach to data principal
c. Sub-section (6): Obligation of data fiduciary to take appropriate remedial action and post details of personal data breach on its website, based on direction from the Authority

Data fiduciaries should also be allowed to take an independent call on whether data breaches should be notified to users or not, unless directed otherwise by the DPA.

Recommendations

a. To avoid ambiguity, timeline for data fiduciary to notify personal data breach to the Authority should be clearly specified in the Bill. This will enable the organizations to design protocol for incident and breach management in accordance with the provisions of the Bill.
b. Further, threshold for factors or criteria for Authority to determine whether personal data breach needs to be notified to the data principal, should also be clearly specified in the Bill to enable organizations to accordingly design their breach notification process.
c. Organizations are of the opinion that the criteria based on which the Authority would direct the data fiduciary to take appropriate remedial action and conspicuously post details of personal data breach on its website should be clearly specified in the Bill, to avoid chances of discriminating against certain organizations. The requirement should be commensurate with the level of potential harm caused by the breach and number of data principal impacted.

Reference: Personal Data Protection Bill, 2018 (Chapter 7: Transparency and Accountability Measure [Section 33]

Issues:

Data Protection Impact Assessment

Section 33 of the Bill links performance of DPIA to class of data fiduciary.

There is an assumption within Section 33 that processing that involves "new technologies" inherently carries a risk of significant harm to data principal and, therefore, a DPIA is required in all such instances before any processing can be undertaken. On the contrary, there is no evidence to suggest that new technologies carry such a risk. Implementing a statutory requirement for engaging a data auditor to undertake DPIA, or reviewing the DPIA with the regulator could delay the adoption and growth of new technologies in India.

Section 33(4) specifies that the data protection officer shall review the assessment prepared and shall submit the same to the Authority in such manner as may be specified, upon completion of DPIA. Organizations believe that if all organizations operating in India submit all DPIAs that are conducted in a year to Data Protection Authority, the Authority will be overwhelmed with large number of DPIAs, which will add significant cost pressure.

Recommendations

DPIA should only be conducted if there is an assessed risk of serious harm under the general intent of Section 33, and not because of the technology that may be used for the processing or characteristic or size of data fiduciary. Further, one of the security consulting organizations recommend that DPIA should cover the group of assets at people, process and technology level.

Mandatory DPIA for new technologies should be removed. Instead a harm-based approach should be adopted. The draft in its current form sends a negative message related to new technologies and heightened privacy risks associated with new technologies which is misplaced, and in fact could slow down adoption of technology solutions.

Organization are of the opinion that requirement to submit DPIAs to the Authority should only be for those assessments, for which the risk to data principals cannot be mitigated. Further, data fiduciary should still be accountable to conduct required DPIAs and maintain appropriate records.

Reference: Personal Data Protection Bill, 2018 (Chapter 7: Transparency and Accountability Measure [Section 34, 35, 38])

Issues:

i. Compliance requirements

Section 34 and 35 states that DPA shall specify the form and method in which data audits and record keeping will be carried out by significant data fiduciaries. These stringent requirements further the problem of complying with the provisions of the Bill by significant data fiduciaries.

ii. Factors for categorization of significant data fiduciaries

Section 38 – This clause provides for the designation of certain data fiduciaries as significant data fiduciaries by the Data Protection Authority (DPA) on the basis of volume and sensitivity of data processed, turnover of the fiduciary, risk of harm or use of new technologies in processing. This designation comes with higher compliance burdens, as significant data fiduciaries are required to register with the DPA, and mandatory compliances of data protection impact assessments, record keeping, data audits, and the appointment of a data protection officer.

However, the factors to categorize significant data fiduciaries are generic in nature, and do not include any specific figures in the context. Hence, the organizations do not have visibility on the applicability of above-mentioned compliance requirements for them.

Recommendations

The law should provide legal recognition to self-regulatory bodies promoted by industry associations to improve internal governance mechanisms in organizations.

a. Industry driven codes of practice, developed through learnings of the market and by industry members, that are principally aligned with legislative intent,
b. A multi-stakeholder process should be utilized to:
    - Define thresholds for designating entities as significant data fiduciaries; and
    - Develop enabling codes of practice for data audit, record keeping and other compliance requirements, which allow flexibility in implementing these requirements.
c. It is not clear why this category of data fiduciaries needs to be created, and we recommend that this be deleted, to avoid detrimental impact such as

- Large employers, who are data fiduciaries because they process data of employees may be unnecessarily categorized as SDF. This category should be exempted altogether
- New technologies as a criterion that requires mandatory enhanced compliance is incorrect and sends a wrong signal. This cannot be the driving criteria for identification of SDF and mandatorily require DPIA.

Reference: Personal Data Protection Bill, 2018 (Chapter 7: Transparency and Accountability Measure [Section 35])

Issues:

Data Audits

The requirement of generating data trust scores should be reconsidered. It could cause much more harm than good, and instead voluntary audits and certification may be relied.

Recommendations

In context of data trust score and data audits, AMCHAM recommends that audit type should assess and address requirements of various similar Standards/Regulations/Acts across IT Assets.

Reference: Personal Data Protection Bill, 2018 (Chapter 7: Transparency and Accountability Measure [Section 36])

Issues:

Data Protection Officer

Section 36: The draft data protection bill has clear guidelines for data fiduciaries to appoint Data Protection Officer for their organization. However, measures to ensure independence of Data Protection Officers, avoiding conflict of interest in the roles and responsibilities and measures for compensating lack of sufficient resource pool (Data Protection Officers) in the country have not been addressed in the Act.

Recommendations

Some organizations propose that following aspects in context of Data protection Officers should be included in the Bill:

a. Independence of Data Protection officers
b. No conflict of interest in the roles and responsibilities
c. Reporting of Data Protection Officers to the higher management

Most members have also recommended that for companies with global operations, it may not be possible to appoint a DPO in India. Hence a senior official who is empowered and knowledgeable with other suitable designation should be acceptable. This flexibility may be provided in the draft law.

CHAPTER 8

Reference: Personal Data Protection Bill, 2018 (Chapter 8: Transfer of personal data outside India [Section 40, 41])

Issues:

i. Restrictions and/or ban on cross-border data transfer

The requirement for data localization has been incorporated in the Personal Data Protection Bill, 2018 to:

a. ensure timely access to personal information by law enforcement bodies
b. prevent foreign surveillance

However, many of the players in Financial Services, IT/ITeS industry are of the view that data localization along with restrictions on cross border data flow would:

a. Impair innovation by raising costs, as this will undermine India's ability to leverage emerging technologies that rely significantly on global networks, like cloud computing, AI.
b. Hamper India's growth agenda, and particularly the competitiveness of IT/ITeS (BPO) industry as well as small and medium enterprises or startups that are increasingly reliant on emerging technologies like cloud computing.
c. Risk driving investments away from India given the onerous data localization and mirroring requirements applicable on all data to which the Act applies.
d. Danger of reciprocal action in other countries will impact Indian IT/ITeS companies if similar restrictive policies are adopted.

ii. Categorization of critical personal data

Uncertainty around categorization of critical personal data in Section 40(2) has received criticism from our members, especially in Financial Services industry. Since, critical personal data could be stored and processed only in India as per section 40(2) of the Bill, the industry is of the view that many of the processes like customer support which rely on follow-the-sun models through call centers located in geographically dispersed locations might be significantly impacted, if financial data is included in the mentioned clause.

This combined with concerns around classification of financial data as sensitive personal data risk placing India at a competitive disadvantage to other financial and data analytic hubs, as the requirement of obtaining explicit consent places an unnecessary bar to processing of data which the financial industry in other countries is not faced with

iii. Mechanism for limited cross-border data transfer

Country adequacy, standard contractual clauses, or intra-group rule requirements would have to be satisfied, even if the consent, or explicit consent (in case of sensitive data) from data principals have been obtained, and vice-versa. These would place significant and onerous requirements on the organizations for cross-border data transfers. This along with localization requirement makes India one of the most restrictive business destination. There is little need for such stringent norms,

that does not enhance either the privacy or security of personal data. There are various models that countries adopt to offer data privacy and security that should be considered.

iv. Authority to exempt the applicability of the Act to Business Processing Units

Section 104 provides authority to the Central Government to exempt applicability of the Act to data collected outside India of data principal who is a foreign national. This section is inserted by the committee to give comfort to back office of foreign companies operating in India. Any delay in notification by the Government will directly disrupt businesses and can potentially endanger outsourcing businesses, should there be a need to seek exemption.

Recommendations

Prior to regulating data flows, it is vital that a systematic policy impact assessment be carried out to map the socio-economic impact of such a move against the intended policy objectives. If deemed necessary post the outcome of such a study, data flows should be restricted conservatively and only where necessary to achieve very specific policy goals concerning national security. Such measures should be limited to clearly defined critical data while being non-discriminatory, least trade restrictive, predictable, and aligned with international best practices. This will allow India to further its national interests while maintaining its standing in the global stage as technology powerhouse from an economic growth, market competitiveness and consumer rights perspective.

i. Restrictions and/or ban on cross-border data transfer

a. The entities should be allowed to maintain data at a location as may be best suited for the business, since information security and data loss is location agnostic.
b. Data owners should have controls in place to ensure all personal data is appropriately protected, remains confidential and is only used for purposes notified to data principals, regardless of the geographic location of data storage.
c. Government should also work to form bilateral relationship with other countries through various global forums to support availability of the data as and when required by the government and regulatory bodies.
d. Further, we may have a list of countries where we may not allow transfer of data, considering the privacy regime in the countries and our bilateral relationships with the countries.
e. Additional regulations or guidelines and safeguards dealing with foreign surveillance of the data principals in the country must be drafted by the Data Protection Authority to ensure that the data is stored in furtherance of the provisions of the Bill.

ii. Categorization of critical personal data

Critical Personal Data should be defined after careful consideration of its impact, and with clear rules and guidance on the essential criteria that is required to be met by te data classified as Critical personal Data. Any such notification should be subject to periodic revision and a comprehensive impact analysis of hard localization must be conducted. Any addition to the list of critical personal data should be carefully weighed

a. Further, cross border transfers should ideally not be restricted, and if they must, the restrictions must be the exception and not the norm. Such data categories that should be accorded such sort of protection should be narrowly defined on the basis of very high risk to the data principal.

iii. Mechanism for limited cross-border data transfer

a. Section 41 should be reconsidered to permit additional efficient mechanisms to enable freer flow of data, with accountability and liability fixed on the data fiduciaries.
b. Other enabling accountability models should be considered, such as transfers by or to 3rd parties who have been accredited under a local or international framework in relation to handing personal data.
c. As per the draft bill, consent is a mandatory requirement for any cross-border flow. We recommend that consent should be one of the conditions and not mandatory and in addition to the other clauses within Section 41(1).

iv. Authority to exempt the applicability of the Act to Business Processing Units

Section 104 may be suitably amended to provide general exemption to back office of foreign companies operating in India. The government may retain the authority to extend the coverage of the Act to such companies by gazette notification.

CHAPTER 9

Reference: Personal Data Protection Bill, 2018 (Chapter 9: Exemptions [Section 45]

Issues:

Research, archiving or statistical purposes

Section 45 of the Draft Bill recognizes the value of processing data for research, archiving and statistical purposes and therefore makes an exception for these purposes. However, the provision requires the DPA to consider whether research purposes are permissible on a case-by-case basis. This unduly delays the carrying out of research, which may ultimately have a negative impact on public interest, especially in cases of medical and scientific research etc.

Recommendations

Data fiduciaries should be allowed to make a determination on whether certain processing fits under the research exception as captured by the test in Section 45(3)

CHAPTER 10

Reference: Personal Data Protection Bill, 2018 (Chapter 10: Data Protection Authority of India [Section 62, 63, 64, 65, 66, 75])

In the interest of innovation and competition, a framework of accountability through self and co-regulation may be propagated via the DPA. Market propelled self-certification/ regulating mechanisms, along with incentivization of voluntary disclosure schemes, to implement the codes of practice mentioned in the Bill may be allowed. The industry should be encouraged to voluntarily adopt global best practices and the DPA may retain the power to intervene only if it believes that there is a failure in market forces to act.

Issues:

i. **Power of Authority to issue directions, call for information, conduct inquiry and action to be taken and compensation claims**
   Sections 62, 63, 64 and 65 empower the regulator to issue directions, call for information, conduct enquiry and take punitive actions pursuant to an enquiry on the data fiduciary and the data processor.

ii. Similarly, under Section 75 the data fiduciary is primarily liable to the data principal for any compensation claims from the data principal. However under 75(5) and 75(6) data fiduciary or data processor can be ordered to pay the full compensation and then recover it from data fiduciary and other data processors.

iii. **Powers and Functions of the Authority**
   Section 60(2) of the Bill specifies that one of the functions of the Authority shall include specifying fees and other charges for carrying out the purposes of this Act. However, organizations are of the view that this could have a significant impact on cost and ease of doing business in India.

iv. **Search and Seizure**
   Section 66(1) of the Bill specifies the powers vested in Authorized Officer, authorized by the Authority. However, such powers require a judicial order to be implemented, and an administrative power with the Officer would not suffice.

Recommendations

Data processors in the industry are of the view that if a compensable loss arises as a direct result of an act or omission of the data processor, the data principal can then exercise its rights to seek recovery or contribution from the data processor. The data fiduciary should be primarily responsible for the personal data that it collects from the data principals, and that the data processor should not underwrite liabilities arising under that relationship. Therefore, provisions wherein a data processor can be ordered to pay the full compensation on behalf of the data fiduciary or other data processors should be deleted. We recommend that compensation should be allocated in proportion to the cause and harm and each should pay be ordered to pay their share.

The Authority may also approve and issue codes of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government.

Organizations are of the opinion that this should include codes of practice submitted by certain large organization as well, which are applicable to their suppliers and distributors. These tend to be more effective than industry, or associations, regulator's code of conduct.

Moreover, the search and seizure powers of the DPA must be regulated through judicial oversight. The standard for initiating search and seizure should be changed from 'reasonable grounds' to 'probable cause' to ensure that there is no undue threat to regular business operations.

CHAPTER 11

Reference: Personal Data Protection Bill, 2018 (Chapter 11: Penalties and Remedies [Section 69])

Issues:

Enforcement/ Liabilities/ Penalties

As per Justice SriKrishna Committee report, the proposed penalties and fines are exorbitant in nature. All these would essentially add to expenses and affecting the SMEs/new businesses and would lead to escape moving to the cloud and make India non-competitive.

Recommendations

The suggested penalties are high and can have excessive impact on smaller players and should instead be proportional based on the harm caused. These penalties should be proportionate in nature relying upon the leak or damage and this ought to be founded on standards of proportionality. Further, Industry opposes the imposition of criminal offence and recommends that the law should provide for civil penalties, keeping in mind the principle of proportionality.

CHAPTER 13

Reference: Personal Data Protection Bill, 2018 (Chapter 13: Offences [Section 90, 95])

Issues:

Offences

Section 90: Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act, obtains/discloses/transfers/offers to sell personal data to another person, which results in significant harm to a data principal, then such person shall be punishable with imprisonment for a term not exceeding three years or shall be liable to a fine which may extend up to rupees two lakh or both. Organizations are concerned with the interpretation of this requirement, since the term 'recklessly' is not clearly defined.

Section 95(1): Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. Organizations believe that such offense would not always have been committed knowingly by the concerned employee, person in charge and responsible to the company.

Recommendations

The provision to punish employee, person in charge and responsible to the company, should be limited to proof of intent for the offence and not just being associated with the company at the time, when the offence was committed. Further, the burden should be on the Authority to prove neglect by concerned personnel. Individual criminal liability is also disproportionate given the existence of civil liability and compensation, and might lead to reluctance on part of data fiduciaries to disclose breaches at the earliest.

Other General Recommendations for the Protection Bill

1. The financial services sector at AMCHAM has recommended to make appropriate changes in the Act, to authorize the group entity to designate one of their group entities as data fiduciary.

   The rationale for the recommendation is as provided below:

   a. The pooled investment vehicles are usually structured in the form of a Trust
   b. The role of the Trustee is limited to supervisory/fiduciary responsibilities and such Trustee companies may not have any employee other than its Board of Directors
   c. The day to day operations of the pooled investment vehicle are contractually entrusted to the investment managers for example, Mutual Funds and Alternative Investment Funds registered with SEBI
   d. As per the proposed provisions of the Act, The Investment Manager will collect data on behalf of the Trustees and the amount of data is huge, the Trustees would be identified as significant data

fiduciary. However, it will be extremely difficult for the Trustees to discharge all its responsibilities under the Act on account of lack of staff members.

2. AMCHAM is of the opinion that sufficient time should be granted to the entities to ensure they are able to put in place privacy compliance framework to comply with the requirements of the Bill.
3. Presently, the Bill effectively provides for 6 months of implementation period after notification of codes of practice by the DPA. The comments should push back very strongly on this timeline and suggest the following timelines instead by stating that the Bill should:
4. Provide for a minimum of 2 years for the implementation of the Bill from the date of issuance of rules, codes of conduct or any other compliance obligations. As already provided for, Chapter VIII (Data Localization and Cross Border Flows) should be notified separately and distinctly from the rest of the Bill. This should occur post extensive public impact assessments and consultation with all stakeholders.
5. Recommend that a minimum compliance time frame of 3 years is included within the language of Chapter VIII in the Bill, which should only kick in post the distinct date of notification of Chapter VIII. The government should have the power to extend this 3-year period if felt necessary post industry consultations.
6. In order to ensure that nothing in the law leads to privacy compromising consequences, a clause should be added to clarify that nothing in the law would compel data fiduciaries to re-identify personal data that has been de-identified from the data principal.