www.pwc.in

At a privacy crossroads

ASSOCHAM INDIA

August 2018

pwc


PROGRAMMING
NEXT
click here for more information

Contents

सत्यमेव जयते

Sudhir Mital
Member
Chairperson

Fair Competition
For Greater Good

भारतीय प्रतिस्पर्धा आयोग
COMPETITION COMMISSION OF INDIA
Hindustan Times House
18-20, Kasturba Gandhi Marg, New Delhi-110 001, INDIA
Ph. : + 91-11-23704630, Fax : +91-11-23704631
E-mail : sudhir.mital@cci.gov.in Web.: www.cci.gov.in

MESSAGE

It is indeed a pleasure to see that ASSOCHAM is leading these important discussions on issues of data protection, privacy and security in the digital age. The Knowledge Report is a timely and useful addition to the repertoire of ideas and discussions in this critical area of public policy.

New business models based on collection and processing of big data shape the digital world today. Development of data mining and machine learning technologies are enabling businesses to offer high-quality and customised products and services at low or even zero prices to consumers. However, big data does not come without a cost. In this digital age consumers have become more vulnerable to loss of control over their data, intrusive advertising and behavioural discrimination. These emerging concerns require immediate policy response.

It is a matter of great satisfaction that India has moved a step ahead in this direction and is at the threshold of establishing a robust data protection framework with the release of the Srikrishna Committee Report on 27th July, 2018. The recommendations provide the contours of data protection architecture of the country ensuring consumer privacy and development of innovative businesses at the same time. It is imperative that regulatory interventional boundaries are set by the legislature to reduce friction between laws dealing with data and issues incidental therewith.

In this regard I would like to express my gratitude to ASSOCHAM for providing a platform for intellectual discussions that hopefully will contribute in shaping a nuanced policy in this area. I hope this Knowledge Report examines these issues from all the different perspectives and help the ongoing discourse to strike the right balance between growth and efficiency of digital platforms and consumer privacy.

I once again congratulate ASSOCHAM for this initiative and wish the Summit all success.

(Sudhir Mital)

Place: New Delhi
Dated: 14th August, 2018

ASSOCHAM
INDIA

THE ASSOCIATED CHAMBERS OF COMMERCE AND INDUSTRY OF INDIA

D S RAWAT
Secretary General

Message

Greetings from ASSOCHAM!

The global economy fuelled by data and information that drive and dominate the commercial activities in today's digital world has severe concerns of data security, privacy and threats. The protection and privacy of data has emerged as focal point for businesses around the world. India's timely alignment with the EU's General data Protection Regulation is the determining factor that may turn the future games and wars of the Global Trade & Business .

Data Protection Bill, 2018, recognises privacy as a fundamental right. It has provisions to protect personal data as an essential facet of information privacy. The objective of the Bill is to balance the growth of the digital economy and use of data as a means of communication between persons with a statutory regime that will protect the autonomy of individuals from encroachments by the state and private entities.

In an effort to deliberate upon key perspectives of stakeholders on the Draft Personal Data Protection Bill, 2018 and discuss the reforms, opportunities and implementation challenges, the chamber has been proactively organizing conferences on the subject. In this order, the **3rd Global Summit on "Data Protection, Privacy & Security – Legal Reforms, Challenges & Opportunities"** is being organized on 24th August, 2018 in Mumbai.

I am pleased to acknowledge and appreciate the valuable contributions made by the expert team of PwC India and ASSOCHAM, Dept. of Fintech, Digital Assets & Blockchain Techonology and Competition Law for bringing out Knowledge Report on the subject.

I am sure that the study and findings published in the report will provide rich insights and adequate knowledge to all the stakeholders.

I wish the participants and stake holders of the summit a great success.

With best wishes,

D.S. Rawat
Secretary General
ASSOCHAM

August, 2018
New Delhi

ASSOCHAM Corporate Office : 5, Sardar Patel Marg, Chanakyapuri, New Delhi-110021
Tel. : +91-11-46550555 (Hunting line) • Fax : +91-11-23017008 / 9 • E-mail : assocham@nic.in • Website : www.assocham.org

1 Foreword

Siddharth Vishwanath
Partner and Cyber Advisory Leader
PwC India

In an age where data and information are fuelling the growth of most of the leading economies, it is extremely important to have a bill which will protect the fundamental rights of individuals. We believe that the draft Personal Data Protection Bill is a step in the right direction, despite having a few rough edges that need to be smoothed out.

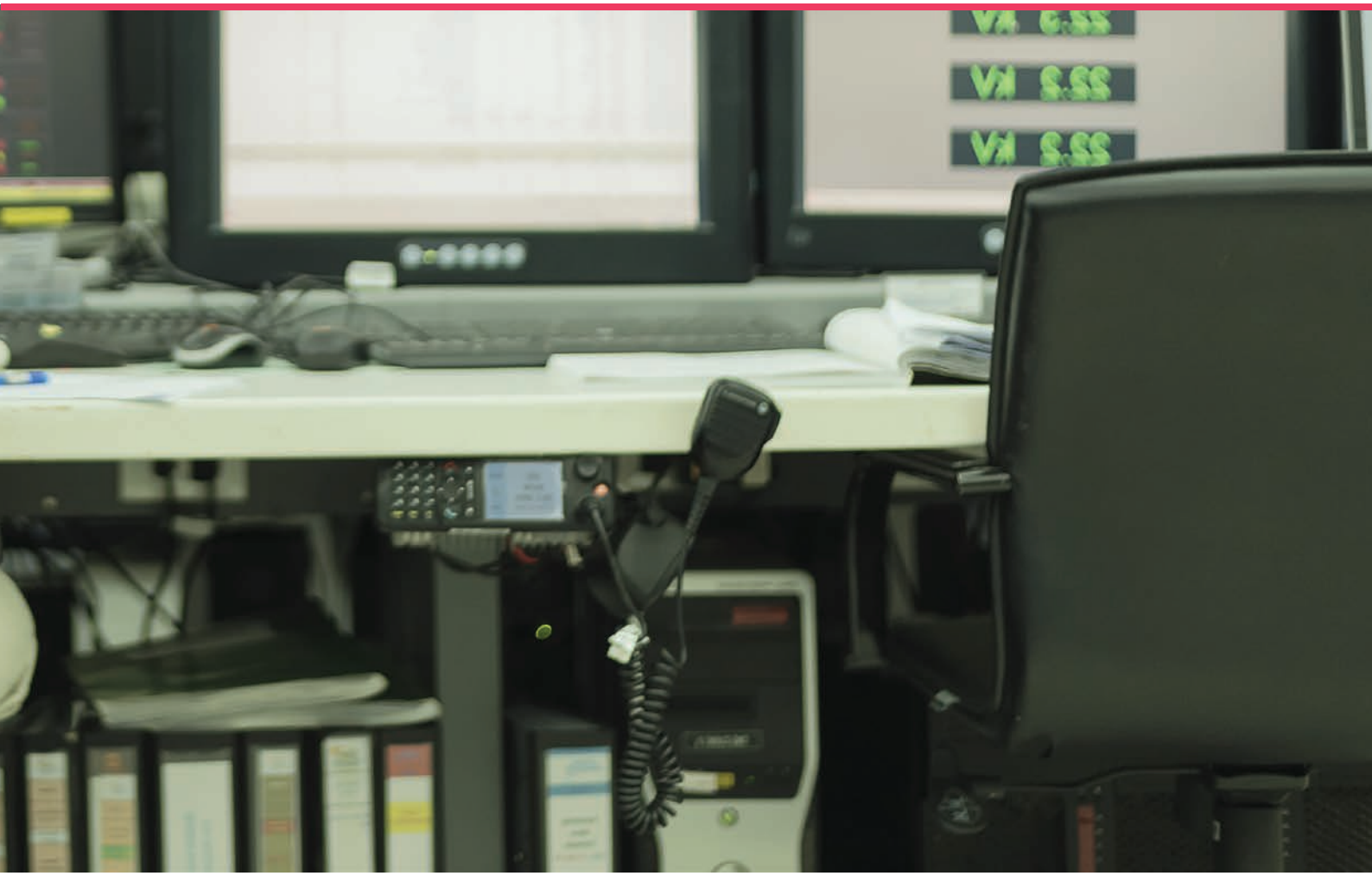
The bill will help bring in the right balance between protecting the rights of the individual and providing adequate authority to organisations to rightfully use the data they capture in a business-enabling manner.

The exclusion of anonymised data from the scope of the bill is likely to fuel innovation. Further, we could see a rise in new technology and start-ups to provide the support (such as consent management) required to comply with the regulation.

The bill provides for exceptions for some of the processing activities and exemptions based on size of the organisation. While the thresholds may be debated, this is a welcome concept.

As the new data privacy and protection regime plays out, timely planning/action will help organisations continue their business as usual and, more importantly, enhance their business reputation.

This report aims to lay out the key imperatives for organisations to align themselves to the robust privacy regime and for the government to establish the right regulatory context.



2 Context

A step in the right direction

Even as organisations in India were coming to terms with the General Data Protection Regulation (GDPR), they found themselves confronted with another regulation—the first draft of India's Personal Data Protection Bill. Last month, Justice B N Srikrishna and his team of legal experts, after a year of research and surveys, tabled the bill for the government's consideration and parliamentary proceedings. The bill considers the challenges of establishing privacy standards in India and seeks to put India at par with the world.

Along with the bill, a report titled 'A free and fair digital economy – protecting privacy, empowering Indians' was released. The report aims to communicate the reasoning behind the inclusions as well as exclusions in the bill.

Needless to say, both the bill and the report have attracted considerable attention and scrutiny, and they mark key developments in the field of data privacy in India following the Supreme Court's recognition of the 'right to privacy' as a fundamental right under the Constitution of India in August 2017.

The proposed Personal Data Protection Bill runs into 112 sections and is very similar to the EU's GDPR; however, it comes with its own challenges and ambiguities. This report touches upon the major privacy areas, the challenges organisations might face and the potential steps organisations should take.

Applicability keeps Indian residents at the core

The bill will be applicable to all organisations incorporated in India and processing (completely or in parts) any personal data on Indian soil. Further, it extends the applicability to any entity incorporated overseas, if it were to provide goods and services (including processing of personal data) to Indian residents or, alternatively, profile data with respect to Indian residents. The bill, in this way, is a positive step in ensuring that a level playing field is established for Indian corporates as well as multinationals wanting to do business in India under the same privacy jurisdiction.

In line with global data protection regulations

The bill is in line with most of the leading global privacy laws and regulations that are currently prevalent, such as the GDPR and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). It touches upon almost all the domains of data privacy such as collection limitation, fair and lawful processing, notices/consents, data subject rights, privacy by design, security safeguards, transfer of personal data, penalties, data quality, privacy incidents or breaches and children's privacy. The bill has also identified the supporting regulatory and administrative framework for enabling the enforcement of its roll-out. This clearly means that the government is very serious about ensuring that entities are forced to include these requirements as part of their normal business operations.

Strong focus on consequence management

Like other global regulations, our bill also proposes a layered approach for levying penalties for non-compliance on organisations which will be tied to an absolute penalty as well as a percentage of the annual global turnover. Depending upon the type of offence or the violations of certain obligations of the bill, the penalties will be levied. This will bring in the necessary seriousness among organisations, whether it is a global company with small operations in India or an Indian company with large operations outside India. The stringent penalty scheme will definitely act as a deterrent for non-compliance and will be one of the key factors which organisations will keep in mind while abiding with the requirements of the bill.

Some considerations

The proposed bill is fairly comprehensive in terms of addressing the key facets of privacy. However, there are certain concerns and challenges with regard to both data principles and organisations handling personal data in the Indian context.

Anonymisation

The proposed bill explicitly states that it will not apply to the processing of anonymised data. However, organisations are required to apply the standards specified by the Data Protection Authority (DPA) for anonymisation. The exclusion of anonymised data will considerably bring down the obligations on entities (both in the private and public sector). In order to prevent harm to specific groups of individuals, the limitation of processing and publishing analysis of anonymised data should be evolved.

Data localisation

The draft bill also proposes that data fiduciaries save a local copy of all personal data that is stored outside the boundaries of India. Although this move could have some negative consequences, as discussed here, it would ensure effective enforcement of the law, reduce bottlenecks in dealing with foreign jurisdictions, and protect national security and interests. Further, in a move focused on protecting national interests and containing the risk of surveillance from foreign states on critical data, the draft bill prevents data fiduciaries from sending 'critical' personal data outside the territory of India. However, what constitutes personal data and 'critical' personal data is a decision that has been left up to the authority. Although the intentions behind the move are good, maintaining data locally will have an impact on businesses across multiple industries that are today cloud led. This will increase the general cost of doing business across industries.

Data processor

The draft bill calls out the data protection obligations, with fair and reasonable processing considered as the core principle. This, in our view, serves as the guiding factor to determine the rightful and lawful processing of data. The data fiduciary/entity is identified as the party responsible for compliance with the Personal Data Protection Act, 2018, and bears the onus of ensuring that data processors fulfil their contractual obligations. However, with no direct regulatory obligation on the data processor, the level of expected compliance will only be as strong as the contract.

As the bill has currently been submitted to the government, it will be interesting to see how it shape up and whether it stays true to its key objective, which is to 'ensure growth of the digital economy while keeping personal data of citizens secure and protected'.

3 Imperatives for organisations

This section covers the imperatives for organisations. As the bill has yet to become an act, organisations have some time before the requirements are enforced in toto. However, this is the right time for companies to start thinking about the future. We believe that organisations should rethink the following aspects: data architecture, data governance, organisation structure, etc., to begin with, and accordingly start the preparation phase.

Ethical obligations towards, customers, employees, third parties and society in general have to be fulfilled regardless of what laws say. Organisations that have a long-standing reputation and focus on customer confidence will drive privacy irrespective of when and how the bill is passed and will continue giving ethics top priority in their business. With ever-growing awareness on privacy, any misuse of data could lead to huge reputational damage.

Take the right call on data collection and consent

Unrestricted and uncontrolled data collection and reuse will have to stop

Companies process a huge amount of information about data subjects each day, be it a small merchant in the consumer market or a multinational industry player. Personal data is collected through multiple ways, not just for business but also for any other future requirement. Organisations will have to limit collection and reuse of data in line with the consent obtained from the data subjects.

It will be challenging for organisations to change the mind-set of collecting and keeping more data than necessary.

Applying the 'need to know/need to have' principle at the time of data acquisition

Unlike in the past where 'need to know/need to do' basis was an internal controls requirement, data that organisations capture will need to pass the same test at the time of being acquired from the data subject.

Data captured for the future use should be weighed against cost of compliance vis–à-vis the upside from cross-sale

Organisations will have to strike a balance between cost/benefits when collecting data for future use. While having data about customers will enable organisations to serve them quickly and cover more horizontal services, the flip side is that all of this will come in at the cost of compliance, which organisations need to be mindful of. Further, legal consequences could mean a direct impact on the bottom line, leaving much at stake.

Consent will be of paramount importance in the data collection process

Organisations will have to draft consent which explicitly calls out the current and future purposes for which the data gathered will be used by them. This will set the tone for how and why the data could be used by organisations. Further, organisations need to draft the consent in modular fashion so as to give customers the choice of not sharing data which may be required for future purposes. Organisations will have to consciously identify data that they are capturing for future needs so as to balance their own business needs and choices of customers. Further, for children, parental consent will have to be obtained and will remain valid till they become majors in the eyes of the law.

When reusing data, consent to repurpose is necessary

Organisations need to ensure that they have obtained the consent to repurpose data as and when such data is being used for purposes other than those specified. Further, the consent will have to be obtained prior to reuse.

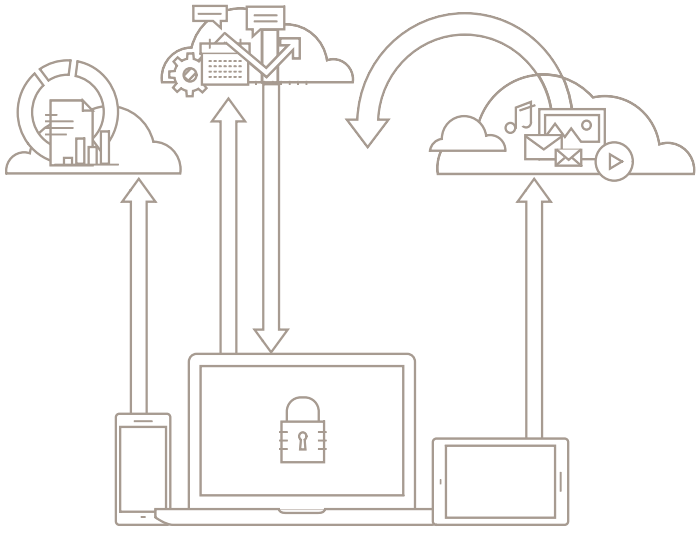
Onus of proving that appropriate consent has been sought will be on the organisation

The data protection laws obligate organisations to obtain consent from the data subject, before or at the time of collecting data. It will be challenging for organisations to prove at a later date that the consent was obtained freely, without any force or in exchange of goods and services other than the purpose of data collection. There has to be an affirmative action by the data subject, such as ticking a box or clicking on a 'continue' link. Further, organisations will have to prove that the consent thus obtained has not been interfered or modified in any manner and is tamper proof. Organisations will have to build a tamper-proof consent storage, archival and retrieval system so that they are able to demonstrate that the consent was obtained prior to data processing and that the timeline and purpose of data usage are in line with the consent obtained. Further, strong measures will have to be taken to protect consent data in order to avoid any downstream legal penalties.

Unlike many international data privacy laws, the draft bill calls out a separate legal ground for organisations to process personal data of employees for purposes necessary for employment.

Multilingual options to be available for notice and consent

The consent will have to be specific to the purpose of processing and the language of consent needs to be simple and understandable by the data subject. This will pose a challenge to organisations as in a diverse country like India, people speak hundreds of languages and it is practically impossible for the data fiduciaries to have the consent printed in all languages. It may be prudent for organisations to have the consent template published in the local state language, along with English and Hindi, depending on the markets they operate in.



Guarantee the rights of the empowered data subject

The right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of information privacy. The power of exercising this right should rest with the individual. The aim is also to protect the privacy of individuals by allowing them determine how their personal data is collected, shared with or used by any entity, public or private.

The bill enforces the right to confirmation and access, right to correction of inaccurate personal data, completion of incomplete personal data, update of out-of-date personal data, right to data portability, right to be forgotten and the right to withdrawal of consent for data subjects.

Building a map of metadata and data for the organisation

We may soon require a data mapping tool to identify where all personal data is stored across the organisation. An individual could exercise his right to seek information about data residency, processing and other details. In order to meet these requirements, organisations will have to implement systems or use technologies to identify the path the data has traversed in the organisation to successfully complete the requests in a reasonable time frame.

Wherever possible, organisations will have to build systems that will become the single source of truth and reduce data duplication/replication, thereby significantly reducing compliance cost.

Digging deep in order to address consent withdrawal requests

Individuals can choose to exercise the right to withdraw the consent. The organisation will have to first identify where the personal data is stored and where it is being processed and delete the data not only from the main systems but also from the back-ups and archived data while maintaining the integrity of the live environment.

Losing or gaining the competitive advantage with data portability

The right to data portability provides an individual full control over her/his personal data which the organisation would have obtained or generated over the years to be transferred to any other organisation, including competition. Organisations face the risk of losing the valuable data of customers to the new service provider or have the opportunity to take advantage of the activities performed by the previous service provider. But, this will definitely benefit individuals, who can move to the new service provider with more ease and probably at a better level of service expectations based on the historical analysis or profile which the past service provider would have generated.

Unbundling of consent and selective consent withdrawal

Data subjects will have the option of selective withdrawal of consent, which means data can be retained only in select systems while it will have to be purged from others.Store only what is necessary

Data purging can no longer be a static time-based rule

Historically, data is deleted when it is no longer required from a regulatory perspective, which is generally a time-based dimension. In the context of the privacy bill, the objective for which the data was collected would take precedence over the time factor. Once the purpose for which the customer provided her/his data is fulfilled, s/he may withdraw consent and the data becomes redundant.

Moreover, storage limitation rules will force organisations to purge data when certain conditions are met. At the same time, they would need to maintain system integrity. In order to achieve this, additional dimensions of the data will have to be captured. It will be prudent to retain only structured data where the data life cycle is short and the data is required for a significantly short duration.

System integrity may be threatened when purging data

Data destruction may compromise system integrity in many legacy and CRM systems as these are not built to allow data destruction or anonymisation. Organisations may have to retune the systems to address these challenges.

Process data for the right purpose

Knowing data attributes and using a common library will be important for secure data processing

Organisations will have to capture the data attributes for personal and sensitive personal data so that when such data is picked for processing by any downstream applications/processes, the requisite security mechanisms are automatically triggered.

Maintaining a master record of consent and purpose of consent will become a norm

Organisations will have to maintain a master list for each individual whose data is processed in its environment to make sure that they are processing data only to the extent to which consent is obtained/available.

Data of children will have to be excluded from analytical routines which could bring harm to them

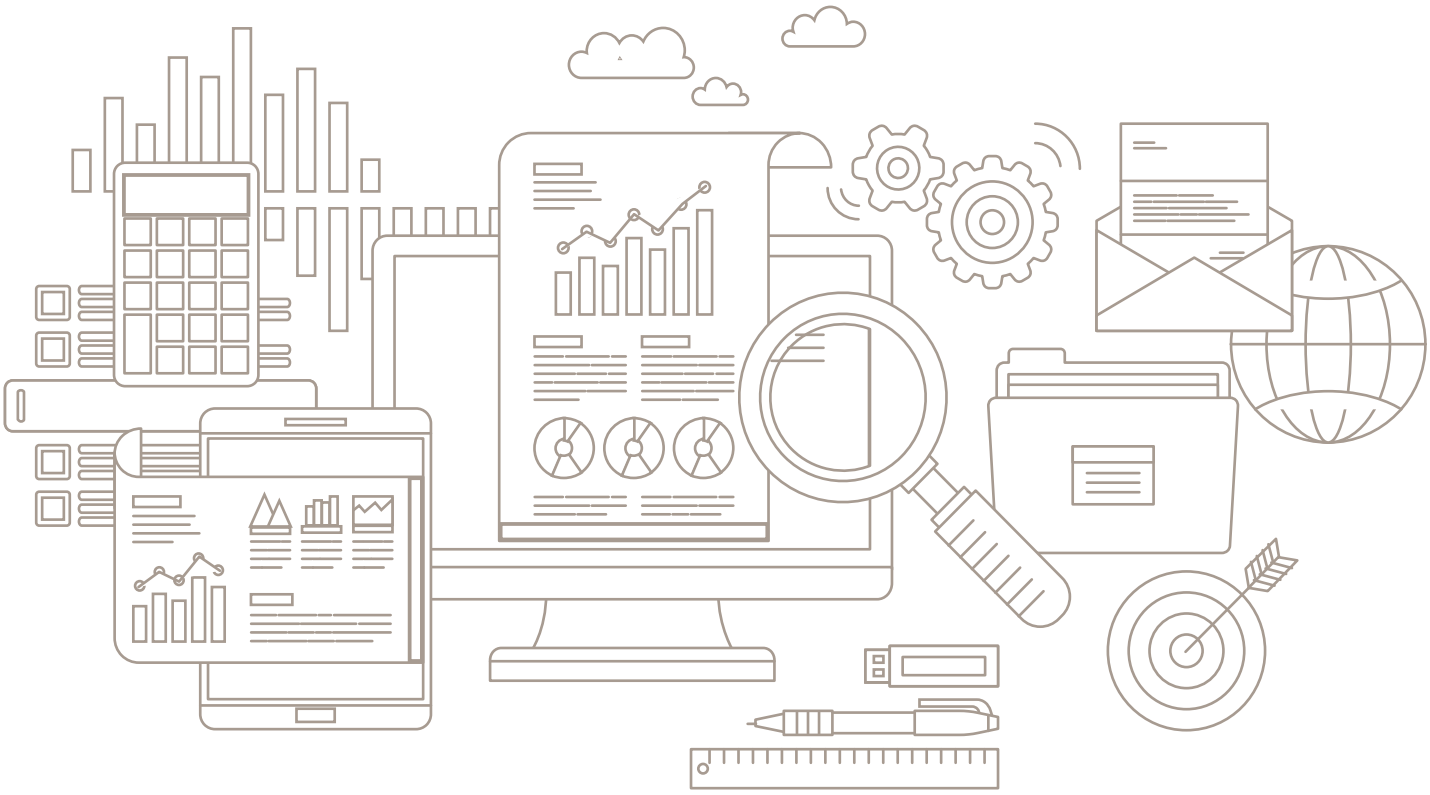
In the case of children, no analytics should be performed which could lead to significant harm to children. Organisations will have to relook at the use cases in their analytics platform and decide on the ones which will need to exclude data related to minors. Any advertisement-driven sales campaign targeted towards children will have to be reviewed.

Reconciliation of data processed and consent available

Organisations will have to periodically reconcile the purpose of the consent available and the actual data processing done in their environment. This will be required to self-assess compliance with the various provisions of the bill. Further, when consent is withdrawn on a selective basis, periodic validations will have to kick in to ensure that these obligations have been met on an ongoing basis.

Anonymising is not a silver bullet

Simply anonymising data will not help comply with the bill. Entities will have to ensure that the data cannot be traced back to individuals post anonymisation.



Managing unstructured data will become extremely expensive

With the introduction of the right to forget clause either in its entirety or selectively, organisations will have to really minimise the usage of unstructured data as it may become an expensive proposition to selectively delete, edit secure and contain data. All manual data-processing touchpoints where data is processed outside of the relational databases will have to be reviewed.

Localise in the era of globalisation and virtualisation

While there are no barriers to information flow in a digital economy, it must at the same time ensure that the rights of citizens and national security are guaranteed. In a worldwide digital economy, data has no boundaries. However, many try to set boundaries for data with concepts such as data sovereignty, whereby data is subject to the laws and governance structures within the nation it is collected. The concept of data sovereignty is closely linked with data security, cloud computing and data localisation. Data localisation builds upon the concept of data sovereignty, which requires certain types of data to be collected, processed or stored inside the country by enacting laws and regulations.

Hybrid structure will evolve to serve localisation requirements

Organisations will have to redraw their technology architecture and implement a hybrid structure to meet the requirements of processing critical data locally. When certain data sets are classified as critical, organisations will no longer have the freedom to process this data outside of India.

Cost of data processing may increase significantly

For organisations which have a global set-up, data localisation will impose a cost burden as they will incur huge costs for duplicating local infrastructure and managing the same. Disaster recovery and other strategies will also have to be relooked at to ensure compliance with the bill.

Cloud installation could prove to be a compliance nightmare

Unless organisations have contractually and through independent assessment confirmed that their cloud service provider does indeed retain at least one copy of data in India through localised replication, they will not be able to comply with the bill. Further, organisations will need to confirm that, at no point during an outage or otherwise, is critical data processed outside of India. From a regulatory perspective, this issue could become the toughest one to navigate over time.

Take a data breach more seriously

Data breaches are a serious business issue

The bill proposes a layered approach for levying penalties for non-compliance on organisations. In order to avoid significant business ramifications due to data breaches, organisations need to outline a well-defined testing mechanism to assess readiness to address any eventualities. Further, they must nominate a competent person, preferably a Chief Data Officer, to communicate with the Data Protection Authority (DPA). The bill proposes a penalty of up to 5 crore INR or 2% of an organisation's total worldwide turnover for the preceding financial year, whichever is higher, in case the organisation fails to meet its obligation to take prompt and appropriate action in response to a data security breach.

Go the extra mile if classified as a 'significant data fiduciary'

An enterprise may be classified as a significant data fiduciary (SFD) based on its turnover or the volume or sensitivity of personal data processed by it. Further, if an enterprise uses new technologies for processing personal data or conducting large-scale profiling and if such processing exposes the data principal to risks, the enterprise will be deemed an SFD. This is a good step by the Indian law to recognise the importance of organisations which are capable of causing significant harm to data principals as a consequence of their data-processing activities and place additional obligations on them.

Data trust score or data audits as a means of competitive advantage

Under the proposed bill, SFDs have to undergo annual data audits using an independent data auditor registered with the authority. The outcome of the audit is a trust score which is assigned to the organisation based on the criteria defined by the Authority. This will make the organisation's data protection practices more transparent and also shift the focus of the organisation from mere compliance to businessWW enablement.

Data Protection Impact Assessment (DPIA) as a tool to pre-empt risk

The proposed bill makes it mandatory for organisations, especially SFDs, to conduct a DPIA for processing activities that may carry a risk of significant harm to data principals. Additionally, SFDs are required to submit their DPIA to the authority, who may either require the organisation to cease processing or implement additional measures. The requirement provides an effective tool for organisations to ensure business interests involved in processing activities are aligned with the privacy interests of data principals.

4 The role of the regulator

In this section, we present our point of view on the expected role of the DPA and measures that will help in implementing and enforcing the law and achieving its intended outcomes.

Independence of the DPA will be the key

For the appropriate functioning of the authority, it is of utmost importance that the authority and its members and officers can function independently. This will ensure that the actions of the government bodies that collect and process personal data are also brought under the ambit of the act. Further, it is important that the authority take an impartial view of the data collection and processing being performed by all entities, including government bodies. Autonomy will be the cornerstone for the successful functioning of the regulatory authority.

Maintaining transparency to build the authority's credibility

One of the best ways to ensure the authority's independence and fairness is to make its functioning absolutely transparent. This is exactly how European regulators of data protection laws function. All enforcement actions, decision notices, audits, advisory visits, overview reports, monitoring reports, self-assessment reports should be easily available on the website of the authority. The data protection law, opinions on it and its interpretations should also be made public for consistent adoption.

Collaboration between public and private sectors

The most pragmatic approach to quickly build capacity and scale is to have a combination of capable personnel and organisations from within the government and private sector working together. One of the options may also be to engage multiple technology and professional organisations to help manage the functioning of the authority. Such collaboration between the public and private sectors could be the key to achieving scale.

Regulator as a guide and advisor

The role of the DPA is not only to govern but also to actively advise and support organisations in adopting the bill. The DPA of India should enable organisations to ensure compliance and provide guidance to and interpret the law for stakeholders. It should act as an advisory body and issue opinions on interpretations of the various requirements of the bill.

Maintaining up-to-date and user-friendly technology, processes and systems

To increase stakeholder trust in the functioning of the authority, it is important that the technology (such as a citizen-facing website), processes and systems that are stakeholder facing are convenient to use and kept updated. Relevant information on reporting the processing of sensitive personal data, empanelment of data auditors, certification process, reporting grievances, checking status, reaching out to adjudicating officers, etc., should be made easily available through various channels. Technology and internal processes should also be aligned to promote ease in communication between stakeholders and the authority.

5 Conclusion

With India going digital and the potential that this move unleashes, the Personal Data Protection Bill is the need of the hour. This is in line with the global trend of increased focus on protecting the rights of citizens with respect to their data. India is moving towards developing a strong regulatory framework to address the challenges of the digital age.

There is traction in various data-intensive sectors such as banking, healthcare and telecom, where the Supreme Court and the respective regulatory authorities (namely the RBI, Ministry of Health and TRAI) are taking a strong stance when it comes to ownership and control of data belonging to individuals.

What this essentially means is that organisations need to shift gears in the way they collect, process, store and share personal data. Having said that, business should see privacy regulation as an opportunity to align themselves for future success and strategic risk management, and not merely to ensure compliance.

Notes

About ASSOCHAM

The Knowledge Architect of Corporate India

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber covers a membership of over 4 lakh companies and professionals across the country. ASSOCHAM is one of the oldest Chambers of Commerce which started in 1920. ASSOCHAM is known as the "knowledge chamber" for its ability to gather and disseminate knowledge. Its vision is to empower industry with knowledge so that they become strong and powerful global competitors with world class management, technology and quality standards.

ASSOCHAM is also a "pillar of democracy" as it reflects diverse views and sometimes opposing ideas in industry group. This important facet puts us ahead of countries like China and will strengthen our foundations of a democratic debate and better solution for the future. ASSOCHAM is also the "voice of industry" – it reflects the "pain" of industry as well as its "success" to the government. The chamber is a "change agent" that helps to create the environment for positive and constructive policy changes and solutions by the government for the progress of India.

As an apex industry body, ASSOCHAM represents the interests of industry and trade, interfaces with Government on policy issues and interacts with counterpart international organizations to promote bilateral economic issues. ASSOCHAM is represented on all national and local bodies and is, thus, able to pro-actively convey industry viewpoints, as also communicate and debate issues relating to public-private partnerships for economic development.

The road is long. It has many hills and valleys – yet the vision before us of a new resurgent India is strong and powerful. The light of knowledge and banishment of ignorance and poverty beckons us calling each member of the chamber to serve the nation and make a difference.

Department Of Corporate Affairs, Fintech & Blockchain Technology

Santosh Parashar
Additional Director & Head
santosh.parashar@assocham.com

Jatin Kochar
Executive
jatin.kochar@assocham.com

Vikash Vardhman
Executive
vikash.vardhman@assocham.com

Abhishek Saxena
Assistant Director
abhishek.saxena@assocham.com

Anish Yadav
Executive
anish.yadav@assocham.com

The Associated Chambers of Commerce and Industry of India
ASSOCHAM Corporate Office:
5, Sardar Patel Marg, Chanakyapuri, New Delhi-110 021
Tel: 011-46550555 (Hunting Line) • Fax: 011-23017008, 23017009
Email: assocham@nic.in • Website: www.assocham.org

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 2,36,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.

About the authors

This point of view has been co-authored by Siddharth Vishwanath, Sriram Sivaramakrishnan, Rushit Choksey and Sunil Prabhakaran. Siddharth Vishwanath is a Partner and leads the Cyber Security Advisory practice for the firm. Sriram Sivaramakrishnan focuses on data privacy and protection within the Cyber Security practice. Rushit Choksey and Sunil Prabhakaran anchor the firm's data privacy and protection programme.

Additional Contributors: Amol Bhat, Gunjandeep Settia and Rajinder Singh.

Contact Us

Sivarama Krishnan
Leader, Cyber Security
sivarama.krishnan@pwc.com

Siddharth Vishwanath
Partner and Cyber Advisory Leader
siddharth.vishwanath@pwc.com

Anirban Sengupta
Partner, Cyber Security
anirban.sengupta@pwc.com

Hemant Arora
Partner, Cyber Security
hemant.arora@pwc.com

Krishna Sastry Pendyala
Executive Director, Cyber Security
sastry.pendyala@pwc.com

Manu Dwivedi
Partner, Cyber Security
manu.dwivedi@pwc.com

PVS Murthy
Partner, Cyber Security
pvs.murthy@pwc.com

Rahul Aggarwal
Partner, Cyber Security
rahul2.aggarwal@pwc.com

Ramanathan (Ram) V. Periyagaram
Partner, Cyber Security
ram.periyagaram@pwc.com

Sangram Gayal
Partner, Cyber Security
sangram.gayal@pwc.com

Sriram Sivaramakrishnan
Partner, Cyber Security
sriram.s@pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
sundareshwar.krishnamurthy@pwc.com

Unnikrishnan P
Partner, Cyber Security
unnikrishnan.padinjyaroot@pwc.com

Venkat Nippani
Partner, Cyber Security
venkat.nippani@pwc.com

Murali Krishna Talasila
Partner, Cyber Security
murali.talasila@pwc.com

pwc.in

GM/Aug2018-14138