KHAITAN &CO ADVOCATES SINCE 1911

ASSOCHAM Celebrating 101 Years

White Paper on Privacy and Data Protection

2 March 2022

Vineet Agarwal
President, ASSOCHAM &
Managing Director, Transport Corporation of India Limited

PRESIDENT ASSOCHAM Foreword

India is experiencing a 'personal data' revolution, as the proliferation of digital services leads to the generation of a significant quantum of personal data. This data is being used by a wide variety of enterprises to deliver value to their users and improve their business operations. The current significant growth in personal data is projected to continue driven by four major consumer forces—rising smartphone penetration, rapid growth in e-commerce, increasing social media penetration, and the emergence of ubiquitous/IoT devices. Technological advancements in data collection, processing, and storage, coupled with government digitization initiatives, are also fuelling the data revolution in enterprises.

In the past, the cyber-attacks, including the WannaCry ransomware attacks, Dyn DDoS and others, on the biggest media company, UK's biggest telecom company, Indian banks, Heathrow Airport, etc., provide testimony to the fact that organizations are constantly under threat. The data leaked included personal information about employees, clients, e-mails between employees, information about executive salaries at the company, and other sensitive information. Such is the scenario today that the world is moving away from physical warfare towards digital warfare. Hence, organizations and countries need to have robust security and privacy frameworks as newer threats evolve in the digital world.

These are exciting times for all stakeholders of the digital ecosystem. The organizations that embrace the change and adopt measures to ensure data security will be better placed for the future. All stakeholders of the digital ecosystem (individuals, organizations and government) need to build security as an integral part of their DNA. The need of the hour is for a cohesive approach to create a secure ecosystem that facilitates business growth and enhances customer experience.

ASSOCHAM is committed to creating more awareness about Privacy, Data Protection and cyber-related issues; this white paper, jointly prepared by Khaitan & Co. and ASSOCHAM, is also a step in that direction. We congratulate the team on their efforts and convey our very best for the **ASSOCHAM Global Privacy and Data Protection Meet 2022**.

Vineet Agarwal

President

ASSOCHAM

Shri Lovneesh Chanana,
Chairman, ASSOCHAM National Council on IT, ITES & eCommerce
and VP, Government Affairs, APJ, SAP

CHAIRMAN ASSOCHAM Foreword

India is on a remarkable growth path fuelled by digital inclusion. As declared by the Hon'ble Prime Minister of India, the 2020s are India's "Techade" and the same is clearly evident by India's growing digital economy which has leapfrogged in the last 2-3 years. In just the second year of the "techade", India's technology industry has acquired revenues worth $200 billion with an IT workforce of nearly 4.7 million. We have seen an exponential increase in start-up unicorns by 160% in last three years. There is an active internet user base of 622 million that is expected to further rise to 900 million by 2025. The building blocks of the $1 trillion digital economy that will enable a $5 trillion Indian economy by 2025, are getting in place.

Digital citizens are a reality today. With improved network penetration and cheap internet costs, India has seen an explosion in data consumption. At 14 GB/person it is one of the highest in the world. Given the large quantum of data produced and consumed, data protection is of utmost importance. Indian citizens are increasingly engaging with new and emerging technologies and new-age applications. These have a "transformative potential" for citizens and the economy, however, there is also the possibility of discrimination, fraud, etc. While the citizens are also becoming increasingly aware of the importance of data privacy and consent, the industry and government must continue to work together to develop frameworks that help citizens utilize their data and provide informed consent for its use and enable companies to harness data and develop public goods for bettering citizen lives.

The government's focus on achieving the $1 trillion target through enabling policies and incentives is laudable. For instance, the recently launched draft data accessibility and use policy provides a framework to harness India's data and possibly create new revenue sources. The success of PLI schemes (for mobile phones, IT hardware) and the recently launched Semiconductor mission reflect the progressive intent and long-term outlook.

As the complex discipline of data protection evolves, collaborative approaches of moving from a regulatory viewpoint to a programmatic viewpoint will be essential. Realising the importance of a wholistic and collaborative data protection environment in the country, we at ASSOCHAM have taken the initiative of bringing different stakeholder groups together on this data privacy summit.

I wish the Summit all the success.

Shri Lovneesh Chanana,

Chairman, ASSOCHAM National Council on IT, ITES & eCommerce and

VP, Government Affairs, APJ, SAP

Shri Deepak Sood
Secretary General, ASSOCHAM

SECRETARY GENERAL ASSOCHAM Foreword

India has taken another step towards realising its dream of becoming a truly digital economy. This progress is aligned with the global direction in which major economies are moving, whereby data protection has emerged as one of the critical areas.

Against the backdrop of an increasingly connected and data-hungry world, we are looking at a paradigm shift in how integrated and intertwined we are becoming with each other. With the increase in the perceived value of personal data, the rise in the use of data for-profit and the advent of technologies such as big data analytics and artificial intelligence, there is a compelling need for Governments around the world to come up with regulations for preventing the misuse of personal information. At the same time, Governments are faced with the challenge of ensuring that the cost of privacy and protection of personal data is not onerous for enterprises. It is being noticed that even developed economies around the globe, with already mature data privacy and protection laws, are undergoing revisions to address the evolving challenges and threats.

Technology is opening vulnerability, with reams of personally identifiable information being collected, stored and shared in a data economy. In response, data regulation in India is evolving rapidly, and data protection, inclusion and privacy have become significant public policy concerns.

Data privacy and the ethical use of data needs to be viewed from the lens of legal and regulatory compliance, along with a focus on ethical and societal aspects of data that can lead to innovative strategies for achieving sustainable success in the marketplace.

I am glad that Khaitan & Co and ASSOCHAM have jointly prepared this detailed white paper for industry leaders and regulators. I congratulate Khaitan & Co and ASSOCHAM IT/ITeS Council for their efforts in preparing this report. We hope this report will serve as a guide for practitioners to implement best practices in data protection.

I convey my best wishes for the success of the **ASSOCHAM Global Privacy and Data Protection Meet 2022**. I hope it provides more insights into the emerging data privacy and cyber-related challenges and solutions to the industry.

Deepak Sood

Secretary General

ASSOCHAM

Supratim Chakraborty
Partner | Corporate and Commercial, Privacy and Data Protection, White Collar Crime

PARTNER KHAITAN & CO Foreword

The growing need for a comprehensive data protection legislation and evolving concerns around the processing of data reverberates louder than ever amidst significant technological disruptions. The digital ecosystem has dramatically transformed over the last few years in India and the sectoral regulators have come up with several guidelines, policies and regulations to address specific concerns around the protection of data and consumer interests.

It is undeniable that at this hour if India aims to harness the growth of digital economy: (i) it needs a comprehensive data protection legislation that lays down a *grundnorm* for regulating processing of data; (ii) it needs to proactively observe and adopt emerging international best practices that are evolving in different parts of the world on fresh approaches for dealing with advancing privacy concerns; and (iii) it needs to initiate and take part in global dialogue on how to make data protection standards interoperable and harmonised with global data protection law standards to ensure seamless transfer of personal data across boundaries.

From an organisation's perspective, businesses that devote considerable resources towards information governance will be able to influence major decisions favourably, including those of its consumers and collaborators. Early movers in this regulatory convergence worldwide will ensure that their organisations stay ahead in the complex and shifting data protection landscape.

I am glad that ASSOCHAM has taken this commendable initiative to facilitate the dialogue among industry leaders, regulators and other stakeholders on multifaceted aspects of regulating data. To further this dialogue, Khaitan & Co and ASSOCHAM have jointly prepared this detailed white paper for all the stakeholders in the digital ecosystem, and I am thankful to ASSOCHAM IT/ITeS Council for their valuable inputs and insights.

I believe in the mandate of this meet and convey my best regards for the success of the ASSOCHAM Global Privacy and Data Protection Meet 2022. I hope that it acts as a whetstone for robust dialogue among stakeholders which culminates into innovative and meaningful solutions for addressing privacy and data protection concerns.

Supratim Chakraborty

Partner

Khaitan & Co

TABLE OF CONTENT

I. Introduction

Inching a step closer to framing a robust data protection regulation for India, the Joint Parliamentary Committee ("**Committee**") submitted its report to the Parliament of India on the Personal Data Protection Bill 2019 ("**2019 Bill**") on 16 December 2021[1], after deliberating for almost two years. With that, the Committee also presented a revised bill, i.e., the Data Protection Bill 2021 ("**2021 Bill**"). Although presently there is no dedicated legislation in India addressing data privacy and data protection, on a sector-neutral basis, the Information Technology Act 2000 ("**IT Act**") and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 ("**SPDI Rules**") regulate aspects of data privacy and protection in India today.

The anticipation of the civil societies and business organisations, in relation to a comprehensive data protection legislation, has reached its zenith since the Hon'ble Supreme Court of India's decision, in *Justice K. S. Puttaswamy (Retd.) vs. Union of India & Ors*[2]. which, upheld right to privacy as a fundamental right that changed the jurisprudence of privacy laws in the country. The verdict pronounced right to privacy as an inalienable, inherent, and natural right that is indispensable to a dignified life and read it into Article 21 of the Indian Constitution.

Witnessing the significant impetus on digital transformation during the Budget 2022, it is undeniable that at this hour, India needs a comprehensive data protection legislation if it aims to harness the growth of digital economy. The digital ecosystem has dramatically transformed over the last few years in India and the sectoral regulators have come up with several guidelines, policies, and regulations to address specific concerns around the protection of data and consumer interests. The 2021 Bill is expected to be laid down before the Parliament of India for its passage later this year.

The 2019 Bill[3] which was primarily modelled along the lines of its European counterpart, the General Data Protection Regulation ("**GDPR**"), mirrored a delicate consensus among the stakeholders on the basic principles governing regulation of personal data. The 2021 Bill has moved slightly away from the GDPR with inclusion of non-personal data, digital media regulations and certification of digital and Internet of Things devices. These are expected to impact businesses in a larger way, leading to demands for fresh industry-wide consultations on the 2021 Bill. The Committee's report also suggested major improvements to the 2019 Bill, such as clarity on timelines, removal of the concept of fixed penalties and emphasis on the growth of start-ups and small businesses, all of which have been largely welcomed by the business organisations.

As a relief to businesses and start-ups, the 2021 Bill has removed the concept of fixed penalties and the Committee, in its report, has recommended that penalties should be subject to a maximum cap and the quantum to be imposed should be decided considering factors such as the size and nature of the business[4]. It also provides the much needed clarity and room for business organisations to realign their business practices and policies with the 2021 Bill as businesses will now have a period of 24 months from the date of enforcement of the law for ensuring compliance[5]. However, this recommendation on the timelines have not been incorporated in the provisions of the 2021 Bill. The Committee also stipulates liability for non-compliance on the independent director / non-executive director in limited cases where the director did not act diligently or where non-compliance occurred with his knowledge[6].

---

[1] Committee Report available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[2] *Justice K. S. Puttaswamy (Retd.) vs. Union of India & Ors.* [Writ Petition (Civil) No 494 of 2012].

[3] Personal Data Protection Bill 2019 available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[4] The Data Protection Bill, 2021, s 57.

[5] Recommendation No. 3, Page 28, by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.

[6] Clause 85, Recommendation No. 83, Page 156, by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.

The 2021 Bill and the Committee's report represents a shift from the basic framework of the 2019 Bill that was centred around regulation of personal data, when it ventures into regulation of social media platforms, hardware manufactures and broadened the scope of the 2021 Bill with the inclusion of non-personal data. The Committee has recommended that the Government should make efforts to establish a mechanism for the formal certification process for all digital and IoT devices[7]. The 2021 Bill stipulates that businesses will now have to demonstrate fairness of the algorithm or method used for processing of personal data[8] and they will not be allowed to deny a request for data portability on grounds of it being a trade secret[9]. The additional obligations on the business organisations have raised larger intellectual property and trade secret concerns.

The Committee also deliberated upon an important aspect of the right of the data principal, i.e., right to control on how their data is dealt with upon their death. The 2021 Bill makes provisions for the data principal to exercise multiple options (i.e., nominate a legal heir, exercise the right to be forgotten or to append the terms of the agreement) in relation to the processing of personal data in the event of the death[10]. The Committee retains the clause where any agency of the Government may be exempted from the application of any or all the provisions of the 2021 Bill. It, however, recommended that the Government should lay down a procedure for oversight that must be just, fair, reasonable, and proportionate[11].

While many of the provisions remain unchanged from the 2019 Bill, there are some significant departures between the two drafts. This White Paper aims to present the key differences between 2019 Bill and the 2021 Bill on a few aspects which can be expected to have significant impact on business organisations and provide suggestions on the way forward.

[7] Clause 49(2)(o), Recommendation No. 10, Page 39, by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.
[8] (n 4), s 23(1)(h).
[9] Clause 19, Recommendation No. 40, Page 78, by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.
[10] (n 4), s 17(4).
[11] (n 4), s 35.

II. Non-Personal Data

1. NON-PERSONAL DATA UNDER THE 2019 BILL

1.1 On a principal basis, 2019 Bill did not regulate non-personal[12] data and excluded anonymised personal data from its scope. Clause 91(2)[13] of the 2019 Bill enabled the Central Government, in consultation with the Data Protection Authority ("**DPA**"), to direct any data fiduciary (akin to data controller under the GDPR) or data processor to provide anonymised personal data[14] or non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies.

1.2 The Srikrishna Committee also deliberated upon issues concerning non-personal data and emerging processing activities that hold considerable strategic or economic interest for the nation but left its regulation to the wisdom of the future committees[15].

2. OBSERVATIONS OF THE COMMITTEE

2.1 The Committee expressed its concern over keeping non-personal data outside the purview of the 2021 Bill. In the Committee's opinion, to define and restrict the new legislation only to personal data protection or to name it as Personal Data Protection Bill is detrimental to privacy and it opined that if privacy is the concern, non-personal data should also be dealt with in the 2021 Bill.[16]

2.2 The Committee felt that a large volume of non-personal data is essentially derived from one of the three sets of data - personal data[17], sensitive personal data[18], and critical personal data[19] -which has either been anonymized or has been in some way converted into non-re-identifiable data. It also felt that it is not possible to differentiate between personal or non-personal data[20] and a lot of times, it is the application of the data that determines whether a data set is personal or non-personal.

---

[12] (n 3), s 3(28), "non-personal data" means data other than personal data.
[13] (n 1), *Section 91(2): The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymized or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.*
[14] (n 1), *Section 3 (28) 'personal data' means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;*
[15] Committee Report available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, Page 13.
[16] (n 4), s 50(6)(o).
[17] (n 14).
[18] (n 1), *Section 3 (36) 'sensitive personal data' means such personal data, which may, reveal, be related to, or constitute—*
(i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15. Explanation.— For the purposes of this clause, the expressions,—
(a) 'intersex status' means the condition of a data principal who is—
(i) a combination of female or male;
(ii) neither wholly female nor wholly male; or
(iii) neither female nor male;
[19] (n 1), *Section 32(2) Explanation— For the purposes of sub-section (2), the expression 'critical personal data' means such personal data as may be notified by the Central Government to be the critical personal data.*
[20] (n 1), Page 25, Para 1.15.8.2.

2.3 Further, the Committee stated that having two DPAs, one for dealing with privacy and personal data and the other dealing with non-personal data will create contradiction, confusion, and mismanagement.

3. COMMITTEE'S KEY RECOMMENDATIONS

3.1 Accordingly, the Committee primarily made the following recommendations in relation to non-personal data:

(a) The application of the 2021 Bill should be extended to non-personal data, including anonymised personal data[21];

(b) Single regulator, i.e., the DPA to regulate both personal and non-personal data[#];

(c) Single legislation for both personal and non-personal data[22];

(d) As soon as the provisions to regulate non-personal data are finalised, there may be a separate regulation on non-personal data in the Data Protection Act[#];

(e) The Central Government may frame policies for the handling of non-personal data including anonymised personal data[#]; and

(f) The 2021 Bill retains the provision around mandatory sharing of non-personal data with the Government. It also introduces incremental concepts pertaining to non-personal data such as "non-personal data breach".

4. ANALYSIS

4.1 Essentially, the Committee offered three justifications for the inclusion of non-personal data in the 2021 Bill - first, non-personal data can also affect privacy; second, it is difficult to distinguish between personal and non-personal data and third, one cannot have two different DPAs to deal with two different kinds of data.

(a) Unsubstantiated privacy concern: The Committee did not offer any rationale as to how non-personal data could potentially affect the privacy of individuals. The only way in which the privacy concern could have some justification is if the protocols for anonymisation are not strong enough, thereby enabling re-identification of personal data. Clause 83[23] of the 2021 Bill already has a strong deterrent in place which makes re-identification a criminal offence.

(b) Exfoliating dissimilitude between personal and non-personal data: In making its case that distinguishing between personal and non-personal data is difficult, the Committee missed the wide swathes of non-personal data that has nothing to do with individuals and no question of re-identification arises in the first place. For instance, military data with armed forces, corporate data with companies, geo-spatial data, reams of multilingual training data

[21] (n 16).
[22] (n 4), s 1(1).
[#] Recommendation No. 2, Page 26, by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.
[23] (n 4), *Section 83. (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable. (2) No court shall take cognizance of any offence under this Act, save on a complaint made by the Authority.*

sets to enable AI-based translation are all now conceptually part of the 2021 Bill as a consequence[24].

The Committee of Experts on Non-Personal Data Governance Framework 2020 ("**NPD Report**") offers an explanation to the issue at Clauses 5.1[25] and 5.2[26] respectively:

(i) Mixed datasets that typically have inextricably linked personal and non-personal data will be governed by the 2019 Bill.[27]

(ii) All personally identifiable data (including anonymized data that has subsequently been re-identified) will be governed by the 2019 Bill and all anonymized data that at the time of evaluation has not been re-identified will be governed by the NPD framework.[28]

(c) Single regulator, half legislation: The fact that there should be a single regulator is a question of regulatory design that would have confronted those who were tasked with regulating non-personal data in the future. It cannot be a reason for making the 2021 Bill an omnibus legislation ahead of time. A single authority and a single legislation are two different matters. Moreover, the goal of a data protection legislation, protecting individuals' privacy, is often at odds with the objective of the NPD Report, which is to generate more value from data.[29] The Committee refers to non-personal data selectively and in a piece meal manner in the 2021 Bill, and it is uncertain as

---

[24] https://vidhilegalpolicy.in/blog/the-data-protection-bill-2021-its-no-longer-personal/

[25] Non-Personal Data Governance Framework, 2020. *Clause 5.1. The Committee evaluated whether there are any overlaps between the regulations proposed for personal data and on-personal data.*
i. The Personal Data Protection Bill, 2019 (PDP Bill) is intended to regulate personal data. It defines personal data as that which is capable of identifying a person. If any data that is personally identifiable is converted to a form that would render it incapable of identifying an individual, it would no longer be personal data and would therefore no longer fall within the remit of the PDP Bill.
ii. This concept is captured within the PDP Bill at Section 2(B) which states that the provisions of the Bill would not apply to any personal data that has been anonymized.
o Anonymization has been defined under the PDP Bill to be the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Data Protection Authority (DPA). The Committee has collated, for reference, some of the basic anonymization techniques in Appendix 4.
iii. Any personal data that has been subjected to this process and consequently anonymized, would become non-personal data that automatically falls outside the purview of the PDP Bill.
iv. The non-personal data regime applies to all data that is not personal data under the PDP Bill or which does not have any personally identifiable information. Since this definition expressly excludes all data that could potentially have been covered by the PDP Bill there is no overlap between the data that is sought to be regulated by the two regimes.
v. Mixed datasets that typically have inextricably linked personal and non-personal data will be governed by the PDP Bill.

[26] ibid, *Clause 5.2. The Committee evaluated what will happen in case there is re-identification from non-personal data.*
i. Non-personal data would continue to be regulated by the non-personal data framework for so long as it remains non-personal data. However, if the individuals whose data constitute the anonymized dataset are re-identified in any manner, either (a) as a result of a subsequent failure of the anonymization technology, or (b) by virtue of the association of the anonymized dataset with other anonymized datasets that together result in re-identification or (c) through any other means of conscious re-identification undertaken by the part of the data fiduciary, such data would no longer be characterised as anonymized data to which the provisions of the PDP Bill will not apply. The dataset will be deemed to have been re-identified and once again fall within the purview of the PDP Bill.
ii. The determination as to whether the PDP framework or the NPD framework applies to a specific kind of data would be determined by the identifiability of that data.
o All personally identifiable data (including anonymized data that has subsequently been re-identified) will be governed by the PDP Bill.
o All anonymized data that at the time of evaluation has not been re-identified will be governed by the NPD framework.

[27] (n 23).

[28] (n 24).

[29] (n 23), *Clause 3.6: The Committee believes that the policy / regulation will lead to the following benefits:*
i. Realizing economic value from use of non-personal data. To generate economic benefits for citizens and communities in India and unlock the potential of social / public / economic value of data.

to how the regulation on non-personal data would harmoniously fit into the scheme of things. Further, there are no specific international precedents for governing personal and non-personal data through the same legislation. The European Union ("**EU**") has, 'Regulation on a framework for the free flow of non-personal data in the EU' for governing non-personal data and it is mutually exclusive from the GDPR.

(d) Impact on businesses: Business organisations have expressed large intellectual property and trade secret concerns over the inclusion of non-personal data in the 2021 Bill, as insights generated from non-personal data and/or anonymised personal data holds immense commercial value for businesses. The Committee did not go into the nuances of non-personal data regulation and its potential impact on businesses.

5. SUGGESTIONS

(a) The inclusion of non-personal data and anonymised personal data in the 2021 Bill should be reconsidered; and

(b) Mandatory data sharing provision in the 2021 Bill should be revisited and necessary safeguards should be included.

III. Data-Localisation and Cross-border Data Transfer

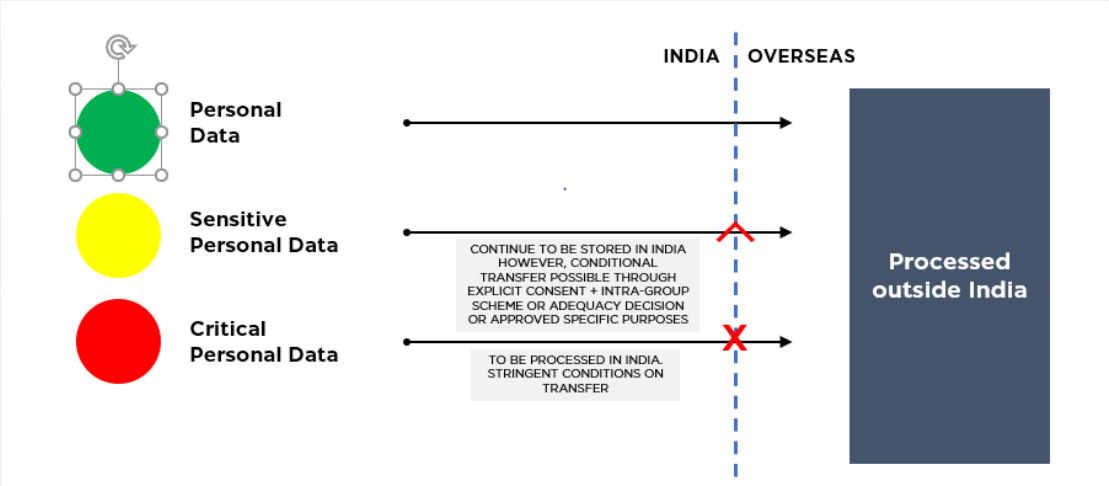
1. CROSS-BORDER DATA TRANSFER UNDER THE 2019 BILL

1.1 The figure below illustrates the overarching framework for the cross-border data transfer under the 2019 Bill.

1.2 The 2019 Bill did not stipulate any additional obligation in relation to cross-border transfer of personal data.

1.3 Sensitive personal data can be transferred outside India, subject to explicit consent of the data principal (akin to data subject under the GDPR) and fulfilment of certain additional conditions such as: (i) through a contract or an intra group scheme approved by the DPA; or (ii) where the DPA has allowed transfer for specific purpose; or (iii) where the transfer is made pursuant to an adequacy decision taken by the Central Government in consultation with the DPA.[30] However, sensitive personal data should continue to be stored in India.[31]

1.4 Critical personal data should only be processed in India. It can only be transferred outside India where such transfer is to a person or entity engaged in the provision of health services or emergency services or where such transfer is made pursuant to an adequacy decision, provided it does not prejudicially affect the security and strategic interest of the State in the opinion of the Central Government.[32]



2. OBSERVATIONS OF THE COMMITTEE

2.1 As per the Committee, data localisation is related to two strategic aspects of data: geographically located data storage and data sharing. Data localization, in broad terms, implies restrictions on the cross-border movement of data and .the local residency / storage of data after processing.

[30] (n 4), s 34.
[31] (n 1), s 33.
[32] (n 1), s 12.

2.2 The recommendations of the Committee on data localisation are rooted in four essential strategic objectives: (a) national security and law enforcement; (b) privacy; (c) employment generation; and (d) bargaining power vis-à-vis the other countries.

2.3 The Committee is of the view that when data is shared between various countries without restrictions, various concerns emerge with respect to national security and growth of local businesses and a country has to balance innovation with the risks associated with cross-border transfer of data. The Committee also put forth their concern that though India has entered into an agreement with many countries under the MLAT framework for the sharing of data for investigation of crimes, the country finds it difficult to get access to data stored in other countries which in turn is delaying speedy delivery of justice and settling of cases. Further, the Committee observed that during the post-COVID-19 times, a huge volume of data is generated due to the offer of services through online platforms and India can attract investment and generate employment opportunities by making use of such emerging trends in the cloud storage market by localising data.

3. COMMITTEE'S KEY RECOMMENDATIONS

Accordingly, the Committee made the following recommendations in relation to data localisation and cross-border transfer of personal data:

(a) The Central Government must take concrete steps to ensure that a mirror copy of the sensitive and critical personal data which is already in possession of the foreign entities be mandatorily brought to India in a time-bound manner#;

(b) The Central Government, in consultation with all sectoral regulators, must prepare and pronounce an extensive policy on data localisation#;

(c) The Central Government's surveillance on data stored in India must be strictly based on necessity, as laid down in the legislation#;

(d) The DPA should consult the Central Government for approvals of transfers of sensitive personal data either through a contract or intra-group scheme or transfers for specific purposes[33];

(e) A contract or intra-group scheme for transfers that are against public policy or state policy will not be approved. In terms of the Committee, an act is said to be against 'public' or 'state' policy, if the said act promotes the breach of any law or is not in consonance with any public policy or State policy in this regard or has a tendency to harm the interest of the State or its citizens[34]; and

(f) An adequacy decision by the Central Government for cross-border data transfer will also include restrictions on the onward transfer of sensitive personal data to any foreign government or agency without the approval of the Central Government.[35]

[33] (n 4), s 34(1)(a).
[34] ibid.
[35] (n 4), 34(1)(b)(iii).

4. ANALYSIS

(a) Expanded role of the Central Government – A desirable approach? The inclusion of the consultative role of the Central Government in granting cross border transfer approvals through a contract / intra-group scheme or for specific purposes is anticipated by the business organisations to make the approval process cumbersome and slow. It has the potential to negatively impact the industries that thrive on the free flow of cross-border transfers of personal data. Further, the addition of the touchstone of 'public' policy and 'state' policy in the approval of cross-border transfer of sensitive personal data will increase the bureaucratic hurdles. Additionally, the pre-condition on onward transfers for granting adequacy decision will result in a lesser number of adequacy decisions.

(b) No onward sharing – Pre-condition for an adequacy decision? In terms of the 2021 Bill, an adequacy decision for cross-border transfer of personal data would also be based on a finding that such sensitive personal data is not shared with any foreign government or agency unless such sharing is approved by the Central Government. This is akin to putting a pre-condition for an adequacy decision.

5. SUGGESTIONS

(a) The consultative role of the Central Government should be removed from approval of the cross-border transfer of sensitive personal data either through a contract or intra-group scheme or transfers for approved specific purposes;

(b) The DPA should be empowered to approve model contractual clauses that govern company's data protection practices to make cross-border transfer of sensitive personal data a seamless exercise; and

(c) The cross-border transfer requirements under the 2021 Bill should be made interoperable and harmonised with global data protection law standards.

IV. Social Media Platforms

1. SOCIAL MEDIA [PLATFORMS] INTERMEDIARIES UNDER THE 2019 BILL

1.1 On a principal basis, the 2019 Bill did not seek to create a regulatory regime for social media intermediaries but lay down specific obligations for social media intermediaries. The usage of the term 'intermediary'[36] in the 2019 Bill was in line with the IT Act.

1.1.1 Social media intermediaries could be classified as a significant data fiduciary by the Central Government in consultation with the DPA depending on the threshold of users and their impact on electoral democracy, security of the state, public order or the sovereignty or integrity of India.

1.1.2 It was incumbent upon the social media intermediaries so classified as significant data fiduciary to enable voluntary verification of user accounts and provide a demonstrable and visible mark of verification to the verified users.

1.1.3 It is important to note that the 2019 Bill was conceived at a time when Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 ("**IT Rules**") was not in force. On regulation of social media intermediaries, the Srikrishna Committee made a similar remark as to the regulation of non-personal data and stated that issues concerning intermediary liability, effective enforcement of cyber security and other philosophical questions require greater deliberation but deferred the regulation to the wisdom of a future committee.

2. OBSERVATIONS OF THE COMMITTEE

2.1 The Committee in its Report noted[37] that, "the present bill is about protection of personal data and social media regulation is altogether a different aspect which needs a detailed deliberation". However, the Committee took cognizance of several concerns around the operations of social media platforms.

2.2 The committee noticed and commented on several problems with social media platforms that range from, "the prevalence of fake accounts" to "instigated people across the globe to plan, organise and execute revolutions, protests, riots and spread violence".

2.3 Commenting on the functions performed by social media intermediaries, the Committee stated that the social media intermediaries perform dual functions of a platform and an intermediary. Expressing the need to regulate social media intermediaries, it remarked that the 'intermediaries' are working as publishers in many situations owing to the fact that they have the ability to select the receiver of the content and also exercise control over the access to any such content hosted by them.

2.4 Juxtaposing digital media with the print and electronic media, the Committee stated that the latter takes responsibility for their content.

[36] Information Technology Act 2000, s 2(w).
[37] (n1), Page 99, Para 2.126.

3. COMMITTEE'S KEY RECOMMENDATIONS

Accordingly, the Committee primarily made the following recommendations in relation to social media platforms:

(a) The social media 'intermediaries' should be designated as 'social media platforms' because, in effect, they act as publishers of content, whereby, they have the ability to select the receiver of the content, as well as control the access to any content posted on their platform[38];

(b) Social media platforms should be held liable for the content from unverified accounts on their platforms#;

(c) No social media platform should be allowed to operate in India unless the parent company handling the technology sets up an office in India#;

(d) A statutory media regulatory authority must be set up on the lines of the Press Council for India for regulation of contents on all such media platforms irrespective of the platform where their content is published, whether online, print or otherwise#;

(e) The Committee dropped the exceptions contained in the 2019 Bill to the definition of social media [intermediaries] platforms without according any sufficient reason[39]; and

(f) The Committee has however retained the provision where social media platforms are required to provide their users with a mechanism to verify themselves voluntarily. This is the sole additional obligation for social media platforms that is reflected in the 2021 Bill[40].

4. ANALYSIS

(a) While the role of social media intermediaries may require reconsideration, a data protection law does not provide the adequate context to do so. Further, there are real concerns around social media regulations, just like there are concerns around cyber security and there would be more pressing concerns in the days to come. A personal data protection legislation is, however, expected to lay down a grundnorm for the regulation of personal data and not provide a quick fix to the issues at hand. Moreover, the remit of the 2021 Bill should only be to the extent where such a platform collects data of its users and processes or shares it with third parties.

(b) Section 79 of the IT Act currently sets out the safe harbor provisions available to social media intermediaries, in conjunction with rules prescribed under the IT Act. It provides insulation to all intermediaries vis-à-vis third-party content on their platforms as long as they follow certain conditions (such as not initiating any transmission, not selecting the receiver of the transmission, and not selecting or modifying the information contained in the transmission) and adhere to their due diligence obligations under the law.

---

[38] (n 4), s 26.
[39] ibid.
Recommendation No. 6, Page 34 by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.
[40] (n 4), s 28(3).

(c) There are rising concerns across the globe on social media intermediaries being assigned the role of 'dumb pipes' that carry all content posted on them without any interference. It is also recognised that they play an active role in selecting the receiver of the content and control access to the content posted on their platform as it is crucial to their visibility and accessibility. While there have been calls for better regulation and increased transparency, it is tenuous to argue that they should be liable for it in the same way a publisher is liable for its content[41].

(d) 'Social media platforms' who have always been treated as intermediaries under extant law, should not be automatically treated as publishers merely because they have the ability to select the receiver of third-party content or can control access to such content. Further, it has to be noted that such platforms may only exercise this ability in pursuance of their legal obligations under Section 79 of the IT Act and the rules thereunder. For instance, the due diligence obligations under the IT Rules enable intermediaries to inform their users that, in the event of non-compliance with their policies, the intermediaries may immediately terminate the user's access and/or take down non-compliant content.

(e) The recommendation is akin to doing away with the safe harbor provision for social media intermediaries. It will fundamentally affect business organisations and as a departure from the 2019 Bill, it would force social media platforms to derogate from a choice-based model for user verification. The recommendations go beyond regulating personal data processing by social media intermediaries and seek to regulate online content being hosted by them.

5. SUGGESTIONS

(a) The 2021 Bill should not create a parallel regulatory regime for social media intermediaries; and

(b) The social media platforms should not be treated as publishers under the 2021 Bill and continue to be treated as intermediaries having safe harbor under the IT Act and the rules framed thereunder.

[41] https://www.news18.com/news/opinion/blue-tick-for-all-jpc-report-on-data-protection-bill-strikes-at-online-anonymity-privacy-4588979.html

V. Data Breaches

1. DATA BREACHES UNDER THE 2019 BILL

1.1 The figure below illustrates the reporting obligations as laid down in the 2019 Bill, to be undertaken by the data fiduciary in the event of any personal data breach. The 2019 Bill did not generally define what a 'data breach' constitutes but laid down a definition for 'personal data breach'[42].

1.2 The 2019 Bill stipulate reporting obligations on the data fiduciary only in the event where such breach is likely to cause harm to any data principal (akin to data subject) and it did not specify any fixed timeline for reporting of such personal data breach. Such breach has to be reported to the DPA by way of a notice.

1.3 Upon receipt of the notice, the DPA may direct the data fiduciary to: (a) report the data breach to the data principal, while taking into account the severity of the harm[43]; (b) take appropriate remedial action[44]; (c) conspicuously post the details of the breach on its website. As per the 2019 Bill, the DPA could also post the details of the personal data breach on its website.

2. OBSERVATIONS OF THE COMMITTEE

2.1 The Committee laid down a detailed analysis of the data breaches and its impact on individuals. It expressed concerns over the subjective discretion of the data fiduciary concerning the reporting of any data breach to the DPA and lack of specific timelines for reporting of such breaches. It stated that there should be a realistic and finite time frame to report a data breach to the DPA.

2.2 The Committee also expressed its concern over the forms and procedures provided for reporting of instances of data breach by the data fiduciary and opined that there

[42] (n 1), *s 2 (29) 'personal data breach' means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data 40 principal;*
[43] (n 4), s 54.
[44] ibid.

should be specific guiding principles to be followed by DPA while framing regulations in this regard.

2.3 The Committee also noted that the term, 'data breach' has not been defined in the 2019 Bill while it has appeared several times in the text.

3. COMMITTEE'S KEY RECOMMENDATIONS

Accordingly, the Committee made the following recommendations in relation to data breaches:

(a) Data Breach has been defined to include personal data breach and non-personal data breach and accordingly non-personal data breaches are also covered under the ambit of 2021 Bill[45];

(b) It laid down a definition for 'non-personal data breach';

(c) All personal data breaches are to be reported to the DPA irrespective of the likelihood of the harm to data principals[46];

(d) Data breaches must be reported to the DPA within 72 hours of becoming aware of such breach;[47]

(e) The DPA may take necessary steps as may be prescribed in case of non-personal data breach[48]; and

(f) Guiding principles for handling data breach:

(i) The DPA should ensure privacy of the data principals while posting the details of the personal data breach#;

(ii) Data fiduciary should be responsible for the harm suffered by the data principal on account of delay of reporting of personal data breach. The burden to prove that the delay was reasonable should lie on the data fiduciary#;

(iii) Data fiduciaries should maintain a log of all data breaches (both personal and non-personal data breaches)#; and

(iv) DPA may use its discretion to authorize temporary order on non-disclosure of details if it does not compromise the interests of data principal.#

4. ANALYSIS

(a) Reporting all breaches: The Committee recommends that data fiduciaries must report all data breaches to the DPA irrespective of any degree of harm to the data principals. This has the potential to overwhelm both, the data fiduciaries and the DPA. The former would have to spend considerable time, effort and resources towards compliance even for inconsequential breaches and the latter would have to deal with a large number of non-serious data breach notices, taking its focus away from the ones requiring attention.

[45] (n 4), s 25.
[46] ibid.
[47] ibid.
[48] ibid.

(b) Fixed timeline: The Committee recommends a hard deadline for reporting data breaches, that is reporting within 72 hours of becoming aware. Businesses are viewing it as a stringent deadline with no room for flexibility. Also, in cases of large-scale security incidents, organisations generally need more time to assess and gather more intelligence around the incident.

5. SUGGESTIONS

(a) Data breach reporting should be limited to circumstances where it poses significant risk or harm to data principals; and

(b) Data Fiduciaries should be obligated to report a data breach without undue delay and where possible such breach should be reported within 72 hours.

VI. Children's Personal Data

1. PROCESSING OF CHILDREN'S PERSONAL DATA UNDER THE 2019 BILL

1.1 The legal nuances surrounding the processing of children's personal data are assuming greater importance and both the Srikrishna Committee and the Committee laid great emphasis on the processing of children's personal data.

1.2 In terms of the 2019 Bill, every data fiduciary has to process personal data of a child in a manner that protects the right of and is in the best interests of the child.[49] It also made the verification of the age of the child and obtaining the consent of the child's parent / guardian pre-requisites for processing children's personal data.[50]

1.3 Interestingly, the 2019 Bill empowered the DPA to classify any data fiduciary as a 'guardian data fiduciary' who had offerings directed at children or processed large volumes of children's personal data. All such guardian data fiduciaries were barred from profiling, tracking, behaviourally monitoring children and their data, or targeting advertisements at children, or processing any personal data that can cause significant harm to the child.[51] The 2019 Bill also made an exception from obtaining the consent of the parent / guardian for a guardian data fiduciary who provides exclusive counselling or child protection services to a child.[52]

2. OBSERVATIONS OF THE COMMITTEE

2.1 The Committee deliberated over several concerns around processing of children's data including lowering the threshold for providing lawful consent for children, doing away with the age verification requirements because it causes additional privacy risks and right of the children to withdraw consent from processing.

2.2 Upon deliberation, the Committee retained the threshold of 18 years for providing lawful consent which is at par with the age of majority in India. The Committee expressed its concern over the absence of any provision laying down the procedure for obtaining the consent of the child on attaining the age of majority (*i.e.*, 18 years). The Committee felt that giving the discretion to the data fiduciary to process personal data of children in their best interest may lead to dilution of the purpose of the provision. Moreover, it felt that there is no added advantage in retaining an additional class of data fiduciary, *i.e.*, 'guardian data fiduciary' and the focus should be on obtaining the consent from the guardian / parent of the child.

---

[49] (n 18), s 16.
[50] ibid.
[51] (n 4), s 16.
[52] ibid.
[#] Recommendation No. 38, Page 74 by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.

3. COMMITTEE'S KEY RECOMMENDATIONS

Accordingly, the Committee made the following key recommendations in relation to processing of children's personal data:

(a) Removal of the phrase, 'in the best interest of', and accordingly data fiduciary has to process personal data of a child in a manner that the protects the right of the child[53];

(b) Data fiduciaries dealing exclusively with children's data, must register themselves, with the DPA[54];

(c) Three months before a child attains the age of majority, the data fiduciary should inform the child for providing consent again on the date of attaining the age of majority[#];

(d) Whatever services the person was getting will continue unless and until the person is either opting out of that or providing a fresh consent so that there is no discontinuity in the services being offered[#];

(e) Removal of the concept of 'guardian data fiduciary' as a separate class. As an effect, all data fiduciaries are now barred from profiling, tracking, behaviourally monitoring children and their data, or targeting advertisements at children, or processing any personal data that can cause significant harm to the child[#]; and

(f) The Committee has added, 'the processing of data relating to children or provision of services to them' as a qualifying factor for the determination of a data fiduciary as a significant data fiduciary under the 2021 Bill.[#]

4. ANALYSIS

(a) Age Limit: The legal age to enter into a contract under the Indian Contract Act 1872, read with the Majority Act 1875, is 18 years. The Committee has retained this threshold for giving lawful consent under the 2021 Bill. The Committee discussed international precedents that provide for lower thresholds for providing lawful consent. As examples, in the United States of America, Children's Online Privacy Protection Act 1998, allows children who are 13 years of age and above to consent, whereas the GDPR mandates 16 years as the threshold, though allowing leeway for states to reduce the age of consent to 13 years. The Committee remarked that, "*We are aware that from the perspective of the full, autonomous development of the child, the age of 18 may appear too high.*" It still retained the high threshold to ensure parity with the legal age to enter into a contract in India. Even after acknowledging the varying level of maturities, the Committee did not carve out any exception for the children between 13-18 years.

(b) Consent requirements: There is a need for revisiting the prism of consent requirements for young persons between the age of 13-18 years. The 2019 Bill had carved out certain exceptions such as those for data fiduciaries who provide exclusive counselling or child protection services to a child.[55] There

[53] (n 4), s 16(1).
[54] (n 4), s 26.
[55] (n 1), s 16.

may be similar instances where the consent may be withheld by parents or guardians but the service maybe nonetheless important for the child.

(c) The 2021 Bill's age verification mandate will likely be challenging to comply with. Determining the exact age of users on a platform could likely require data fiduciaries to ascertain and verify the age of all users in order to identify users under 18 years and then seek parental consent. This will likely be an expensive, intensive, and technically cumbersome compliance obligation that is at odds with the 2021 Bill's data minimisation principle.

(d) Age-gating: Further, in terms of the 2021 Bill, all data fiduciaries are now barred from profiling, tracking, behaviourally monitoring children and their data, or targeting advertisements at children, or processing any personal data that can cause significant harm to the child.[56] As a consequence, all data fiduciaries, irrespective of their level of engagement with children or children's offerings will have to verify the age of its users and it has the potential to age gate the internet.[57] The blanket prohibition on profiling may also render the age-verification and consent obligations infructuous. One of the most effective ways of verifying a user's age is by monitoring their activity on relevant platforms. Under the 2021 Bill, such monitoring also risks being labelled as 'profiling', ultimately rendering the proposed age verification framework inefficient.

(e) Blanket ban on processing activities: Business organisations are concerned about the blanket ban on certain processing activities. The primary contention of the business community is that JPC has retained a generic ban on 'profiling', 'tracking', 'monitoring', 'targeting advertisements' and 'processing' in relation to children's personal data and has failed to take into account the nuances and the significance of each activity. Further, this could also complicate things in a prejudicial manner to the child when data fiduciaries would be refrained from targeting content towards children and young persons. While there is legitimate reasoning behind regulating targeted ads at children to prevent exploitation, a blanket prohibition might also entail harmful and unintended consequences. Such prohibition will make it difficult for companies to ensure the safety of young users on their platforms, and might leave them vulnerable to undesirable and harmful experiences such as grooming. Prohibition on profiling will also prevent data fiduciaries from targeting positive advertisements and resources (such as those related to mental health, suicide prevention, etc.) to children.

5. SUGGESTIONS

(a) The age of providing consent in terms of the 2021 Bill should be brought at par with international standards of 13-16 years;

(b) Specific carveouts for parental consent requirements should be provided especially for children between the age of 13-18 years; and

(c) Blanket ban on processing activities should be reconsidered and ban should be restricted to activities that are proven to cause significant harm to children.

[56] (n 4), s 16.
[57] ibid.

VII. Conclusion

The Committee's report and the 2021 Bill are monumental developments in the data protection framework discourse of India. The business organisations have expressed both their concerns and consensus on the recommendations of the Committee. In light of our discussion in this White Paper, the 2021 Bill presents several dichotomies, which will need to be ironed out before the 2021 Bill is tabled before the Parliament for its passage. We hope that the concerns of the larger business community are factored in and consultations with stakeholders are conducted on key aspects of the 2021 Bill, before it is tabled before the Parliament.

VIII. Abbreviations

i. # : Recommendations by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019 that have not been reflected in the Data Protection Bill 2021
ii. 2019 Bill: The Personal Data Protection Bill 2019
iii. 2021 Bill: The Data Protection Bill 2021
iv. Committee: Joint Parliamentary Committee on the Personal Data Protection Bill 2019
v. DPA: Data Protection Authority
vi. EU: European Union
vii. GDPR: General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
viii. Indian Constitution: The Constitution of India, 1950
ix. IT Act: Information Technology Act, 2000
x. IT Rules: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
xi. MeitY: Ministry of Electronics and Information Technology, Government of India
xii. MLAT: Mutual Legal Assistance Treaty in Criminal Matters
xiii. NPD Report: Report by the Committee of Experts on Non-Personal Data Governance Framework, 2020
SPDI: Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

About Khaitan & Co

Khaitan & Co was founded in 1911 and is among India's oldest and most prestigious full-service law firms. It is also one of the largest, with over 850 professionals and 185 partners and directors. The firm's teams, comprising a powerful mix of experienced senior lawyers and dynamic rising stars in Indian law, offer customised and pragmatic solutions that are best suited to their clients' specific requirements. The firm acts as a trusted adviser to leading business houses, multinational corporations, financial institutions, governments, and international law firms. From mergers and acquisitions to intellectual property, banking to taxation, capital markets to dispute resolution, and emerging areas like white-collar crime, data privacy and competition law, the firm has strong capabilities and deep industry knowledge across practices. With offices in New Delhi, Noida, Mumbai, Bengaluru, Chennai and Kolkata, the firm also has capabilities in overseas markets via its country-specific desks and robust working relationships with top international law firms across jurisdictions. The firm opened its first international office in Singapore last year.

About ASSOCHAM

The Associated Chambers of Commerce & Industry of India (ASSOCHAM) is the country's oldest apex chamber. It brings in actionable insights to strengthen the Indian ecosystem, leveraging its network of more than 4,50,000 members, of which MSMEs represent a large segment. With a strong presence in states, and key cities globally, ASSOCHAM also has more than 400 associations, federations and regional chambers in its fold.

Aligned with the vision of creating a New India, ASSOCHAM works as a conduit between the industry and the Government. The Chamber is an agile and forward-looking institution, leading various initiatives to enhance the global competitiveness of the Indian industry, while strengthening the domestic ecosystem.

With more than 100 national and regional sector councils, ASSOCHAM is an impactful representative of the Indian industry. These Councils are led by well-known industry leaders, academicians, economists and independent professionals. The Chamber focuses on aligning critical needs and interests of the industry with the growth aspirations of the nation.

ASSOCHAM is driving four strategic priorities - Sustainability, Empowerment, Entrepreneurship and Digitisation. The Chamber believes that affirmative action in these areas would help drive an inclusive and sustainable socio-economic growth for the country.

ASSOCHAM is working hand in hand with the government, regulators and national and international think tanks to contribute to the policy making process and share vital feedback on implementation of decisions of far-reaching consequences.

In line with its focus on being future-ready, the Chamber is building a strong network of knowledge architects. Thus, ASSOCHAM is all set to redefine the dynamics of growth and development in the technology-driven 'Knowledge-Based Economy. The Chamber aims to empower stakeholders in the Indian economy by inculcating knowledge that will be the catalyst of growth in the dynamic global environment.

The Chamber also supports civil society through citizenship programmes, to drive inclusive development. ASSOCHAM's member network leads initiatives in various segments such as empowerment, healthcare, education and skilling, hygiene, affirmative action, road safety, livelihood, life skills, sustainability, to name a few.

Deepak Sood
Secretary General
ASSOCHAM
sg@assocham.com

The Associated Chambers of Commerce and Industry of India
4th Floor, YMCA Cultural Centre and Library Building,
01 Jai Singh Road, New Delhi – 110001
Website: www.assocham.org

KHAITAN &CO ADVOCATES SINCE 1911

CELEBRATING 110 YEARS

ASSOCHAM
Celebrating 101 Years

Bengaluru ▪ Chennai ▪ Kolkata ▪ Mumbai ▪ NCR
Singapore

www.khaitanco.com ▪ www.assocham.org