25 January 2022

To,

Shri Ashwini Vaishnaw
Minister, The Ministry of Electronics and Information Technology (MeitY)

Shri P.P. Chaudhary
Chairperson, Joint Committee on the Personal Data Protection Bill

Shri B.N. Mohapatra
Joint Director, Joint Committee on the Personal Data Protection Bill

Re: Asia Internet Coalition (AIC) Submission on Joint Parliamentary Committee's Report on the Personal Data Protection Bill

I am writing on behalf of Asia Internet Coalition (**AIC**). AIC is an industry association that represents leading global internet companies on matters of public policy. To further its mission of fostering innovation, promoting economic growth, and empowering people through the safe and open internet, AIC would like to present our comments on the **Joint Parliamentary Committee's Report on the Personal Data Protection Bill, 2019**.

The Joint Parliamentary Committee (JPC) on 16 December 2021 laid down its report on the Personal Data Protection Bill 2019 (PDP Bill 2019) before the Parliament of India (Report). The JPC has proposed a revised version of the PDP Bill 2019, i.e., the Data Protection Bill, 2021 (DP Bill 2021). We extend our appreciation to the JPC for its efforts in holding detailed public consultations while reviewing the DP Bill 2021 in order to make it at par with global laws, such as the European Union (EU)'s General Data Protection Regulation (GDPR). We note that the Report lays great emphasis on the promotion of ease of doing business and the development of India's digital economy. Accordingly, the JPC has recommended transitional provisions so that relevant entities have sufficient time to ensure compliance. The JPC has also appreciably recommended provisions relating to regulatory sandboxes, the promotion of start-ups, etc.

However, before the DP Bill 2021 is taken up by the Ministry of Electronics and Information Technology (MeitY) before the Parliament, we would like to highlight certain concerns **(see table in Appendix A)** we have with the draft law. We request the MeitY to consider these concerns and request for a discussion on the same with the MeitY at the earliest.

As a next step, we look forward to engaging in additional consultations with the MeitY on the issues highlighted by us in the table below, before the DP Bill 2021 is considered by the Parliament.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Cc:

- Shri Rajeev Chandrasekhar, Minister of State for Electronics and Information Technology
- Shri Ajay Prakash Sawhney, Secretary, The Ministry of Electronics and Information Technology (MeitY)
- Shri S. Gopalakrishnan, Additional Secretary to Prime Minister, Government of India
- Dr. Hiren Joshi, Office on Special Duty (OSD), Communications & Information Technology, Government of India
- Shri Amit Khare, Advisor to Prime Minister, Government of India
- Dr. Rajendra Kumar, Additional Secretary, The Ministry of Electronics and Information Technology (MeitY)

Appendix A

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
1.	**Non-personal data:** ● The JPC has renamed the "Personal Data Protection Bill" as the "Data Protection Bill", since it has recommended governing the processing of non-personal data (**NPD**) within the same law and since it has	**Issue:** ● We believe that there are fundamental and conceptual differences between PD and NPD. The regulatory intent also differs. Thus, both data types should not be covered under the same legal framework.

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
	introduced relevant changes to the text of the DP Bill 2021. According to the JPC, the same regulator, i.e., the Data Protection Authority (**DPA**) should regulate NPD as well. ● We note that the JPC's rationale for this broadening of scope stems from its opinion that during processing of mixed datasets it is difficult to distinguish between personal data (**PD**) and NPD. ● The DP Bill 2021 empowers the Central Government to mandate any company operating in India to share proprietary anonymized personal data or NPD with it for the broadly worded purpose of better targeting of service delivery and formulation of 'evidence-based policies'.	● The fundamental outlook and function of the regulator towards implementation of the DP Bill 2021 for the (i) protection of personal data and (ii) as a framer of policy for use of NPD for public benefit, are different. The capabilities required of the regulator for PD and NPD are different. Hence, it is important to have separate frameworks and regulators for the governance of personal data and NPD. **Comments:** ● If at all a framework for NPD regulation needs to be developed, it should be in the form of a separate and distinct framework. ● NPD (including selective prohibitions such as Section 92) should not be included within the DP Bill 2021 – a law which, in substance, continues to primarily govern PD and has protection of user privacy / PD as its core intent. We elaborate as follows: - A framework that seeks to regulate PD would focus on the privacy of individuals to ensure that there is no misuse or harm arising from processing of their PD and to set appropriate standards for businesses to follow while implementing privacy safeguards. Similarly, the DPA as a regulator for PD would primarily be tasked with protecting the interests of data principals, preventing misuse of PD, ensuring adequate data protection, etc. - In case of NPD, there are no privacy concerns to be addressed since such data does not relate to or identify individuals. The focus of any framework that may govern NPD would be to ensure and promote use of NPD for Indian economic interests, enable free flow of NPD, etc. – an approach similar to the

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		European Union's approach in separately regulating NPD. - Lastly, we would like to bring notice to the fact that since mandatory sharing of NPD has been retained by the JPC under Section 92(2) of the DP Bill 2021, this provision may create regulatory hassles and uncertainty for businesses. This is because if such mandatory sharing mechanisms are implemented without sufficient safeguards to companies' intellectual property rights, it could impact free-flow of data, particularly NPD, in free market economies. This provision also risks violating India's obligations under the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), which requires the protection of secrecy of commercially valuable information and preventing its disclosure without the consent of the person maintaining its secrecy. - Therefore, in light of these fundamental differences, regulation of NPD under the DP Bill 2021 and under the same regulator (DPA) should be completely avoided and Section 92 of the Bill should be excluded.
2.	**Strict data localisation requirements:** ● We note that the JPC has retained all data localisation requirements under Section 33 vis-à-vis sensitive PD (**SPD**) and critical PD (**CPD**), albeit with additional compliances, despite stakeholder requests to reconsider the same. The JPC has recommended that India should move towards complete data localisation gradually. ● Separately, we note that the JPC has recommended that mirror copies of SPD and CPD already in possession of foreign	**Issue:** ● The data localisation requirements under the DP Bill 2021 and the JPC's recommendations in relation to the same are onerous and will hamper the ease of doing business. **Comments:** ● At the outset, robust cross-border data flows are essential for the success of any emerging economy in this era of globalisation. All of which will be hampered due to restrictive data localisation requirements under the DP Bill 2021.The proposed obligation under the DP Bill

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
	entities should be "mandatorily" brought back to India.	2021 would require companies to localize mixed datasets for compliance purposes. Our concerns with these requirements are: - Requiring local storage of SPD can increase the costs of companies and start-ups, who will have to shift all data to data centres and storage systems in India. Further, there are other technical difficulties that exist vis-à-vis localisation. For instance, the scope of SPD is not fixed and clear-cut as the Central Government can notify additional categories of SPD. Further, companies having mixed and inseparable data sets of SPD and PD or SPD and NPD (as the case may be) would have to completely localise such datasets for compliance purposes. Companies may not always be able to separate mixed datasets that have elements of both SPD and PD, or SPD and NPD. Additionally, localisation can lead to other privacy concerns. This is because it is currently uncertain as to whether only SPD collected by a data fiduciary should be stored in India or if SPD voluntarily generated by users on a data fiduciary's platform should also be stored in India. In case of the second situation, data fiduciaries would have to closely monitor all activity of their Indian users to assess compliance. Localisation can also lead to added cybersecurity risks. Concentrating data storage systems in India may also create a single point of vulnerability whereas distributing servers across the world may help preserve business continuity against system infiltration or system failures. - CPD transfers may be allowed where appropriate safeguards - certifications or adequacy mechanisms etc are in place, the categorisation of CPD is also uncertain in the absence of a definition. This raises substantial uncertainty for compliance.

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		- Since localisation is a pre-planned investment-heavy activity, there should not be ambiguity in the law on what datasets constitute CPD and SPD (as highlighted above). Thus, these definitional issues relating to CPD and SPD require immediate clarification. - Lastly, while the JPC has recommended that mirror copies of SPD/CPD be brought back to India, this recommendation is retrospective in nature. The MEITY should avoid considering such a recommendation since retrospective application of data localisation obligations which were not in force when the SPD/CPD may have been collected cannot legally and constitutionally be enforced. Further and at the very least, we urge the MEITY to explore soft localisation as an option vis-à-vis enabling companies to store mirror copies of SPD outside India as this will improve ease of compliance under the law.
3.	**Additional regulation of cross-border data transfers:** ● Under Section 34 of the DP Bill 2021, the JPC has suggested amendments to increase Central Governmental involvement in all SPD related cross-border transfer decisions taken by the DPA.	**Issue:** ● Cross-border transfer decisions should be free from executive or political interference, and should ideally be minimally regulated. ● Conditions for privacy safeguarding cross-border data flows must be based on established legal principles, and technical feasibilities / requirements. **Comments:** ● Increasing the role of the Central Government in cross-border transfer decisions undertaken by the DPA will erode and undermine the regulator's independence. Far-reaching Government involvement in the framing of industry standards on data localisation or hindering cross-border

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		transfers will compound the risks and costs of doing business in India. This, coupled with the requirement of obtaining Central Governmental approval to further share data with foreign governments or agencies of any country to where cross-border transfer has already been approved upon an adequacy decision, can result in transfer decision delays, and thus substantially increase the caseload of DPA, as well as impact the business operations of companies that rely on cross-border transfers of data. ● Placing restrictions on cross-border data flows is likely to result in higher business failure rates, introduce barriers for start-ups, and lead to more expensive product offerings from existing market players. Ultimately, the above mandates will affect digital inclusion and the ability of Indian consumers to access a truly global internet and quality of services. ● Separately, we would like to express our concern over the explicit consent requirement for every SPD related cross-border transfer. We believe that individuals should not be repeatedly burdened to make informed decisions on such transfers. This can lead to consent fatigue and may render the process of obtaining consent futile. ● Therefore, we urge MEITY to reconsider the provisions of Section 34 and account for the following: - Instead of requiring that all cross border transfer decisions be approved by the DPA in consultation with Central Government, the DPA should be empowered to approve model contractual clauses that govern companies' data privacy protection practices so that individual's data is safeguarded at all times, including during cross-border transfers. - Additional consent for cross-border transfers appear irrelevant to the Bill's overall intent

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		of effective data processing, since the processing (even in the absence of this additional consent) can only take place based on permitted grounds of processing. Instead of mandating explicit consent from individuals for cross-border transfers, alternate options like requiring a company to demonstrate to an independent third-party certifier the robustness of its privacy practices (including security) can be implemented. After certification, cross-border transfers need not require consent.
4.	**Social media companies as publishers:** ● The JPC distinguishes between "social media intermediaries" (**SMIs**) and "social media platforms". This distinction is based on the reasoning that some platforms are not intermediaries and act as "publishers" if they have "ability" to select who can receive content and can exercise control over access to such content. ● According to the JPC, "social media platforms" entities should be held responsible for the content on their platforms, especially for content from unverified accounts.	**Issue:** ● At the outset, the DP Bill 2021 is a data protection legislation and intermediaries are already regulated comprehensively under the *Information Technology Act, 2000* **(IT Act)**. Isolated mandates in the DP Bill 2021 for intermediaries is not only beyond the scope and preamble of the DP Bill 2021 but will also cause regulatory confusion and negatively impact ease of doing business. ● The new categorisation of social media businesses as "platforms", accompanying certain obligations is beyond the scope of the DP Bill. This mandate is globally unique and does not find mention in any other data protection regulation worldwide. ● The distinction between SMIs and platforms, and their treatment as "publishers" as reflected in the JPC's commentary in its Report, goes against the safe harbour principle established under Section 79 of the IT Act. **Comments:** ● It is crucial that the notion that social media platforms be treated as publishers be kept out of the scope of data protection regulation.

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		Intermediaries are already regulated under the IT Act and its rules, primarily, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**IT Rules**). Under the IT Act, safe harbor is available to all those intermediaries – including SMIs – for third-party content hosted by them as long as they follow the relevant conditions stipulated therein and adhere to their due diligence obligations under the IT Rules. ● The additional parallel categorisation of social media companies as "SMPs" is out of alignment with global laws on intermediary regulation or more pertinently, data protection. ● Social media businesses should not be automatically treated as publishers merely because of their ability to control access to content or select the receiver of content. This ability may be inherent to many of them, and they may have to exercise it in order to continue to avail safe harbour under the IT Act by adhering to their due diligence obligations under the IT Rules. Instead, it makes sense to retain the traditional understanding of a publisher as an entity that individually selects and makes available a specific piece of content through a distribution outlet. Social media outlets that facilitate access to content published by *others* on their platform are not themselves publishers, regardless of the curation and promotion their outlets may offer. ● This should not, by itself, prejudice such companies and render them liable to be considered as publishers. Not only will this conflict with principles established under extant law, but in the worst case, could render safe harbour completely infructuous. This will, in turn, raise concerning consequences for India's digital ecosystem.

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		● Moving away from the established norm of treating certain entities as intermediaries who have safe harbour and regarding them as publishers who can be held liable for third-party content will gravely harm their business operations – all of which have been structured according to Section 79. This can also lead to businesses being over-cautious regarding third-party content on their platforms, thereby affecting the freedom of speech and expression of their users. ● The JPC report notes that "*the present Bill is about protection of personal data and social media regulation is altogether a different aspect and which needs a detailed deliberation.*" We agree with the Committee on this point and submit that isolated intermediary liability and content regulation provisions in a data protection law will cause significant regulatory overlap, overreach and uncertainty. This will, in turn, impair the ease of doing business in India. ● Importantly, the criteria for safe harbour and SMP regulation is beyond the scope of the DP Bill 2021, as has been explicitly recognised by the JPC in the main text of the Report. Accordingly, recommendations relating to SMPs and the scattered provisions of the DP Bill 2021 governing them including definitions of 'intermediary' and 'platform' should be separately deliberated with relevant stakeholders viz. extant laws and not be introduced as part of the DP Bill 2021.
5.	**Definition of SPD and CPD** ● The definitions of personal data (PD), critical personal data (CPD) and sensitive personal data (SPD) and NPD remain the same as in the 2019 Bill.	**Issue:** ● SPD was defined broadly to include personal data that "*may*" reveal, be related to or constitute the types of sensitive information listed in Section 3(41) of the DP Bill 2021. In comparison, the corresponding definition of

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		SPD in the GDPR is an exhaustive list of types of sensitive information. ● Furthermore, the scope of CPD is left undefined, vague, and to the sole discretion of the Central Government. CPD entails stringent data localisation obligations. **Recommendations:** ● Regulatory ambiguity in definitions denies a stable policy and compliance environment to service providers in India. Processing (which includes storing) CPD *only* in India will entail major planning and investments from companies, which requires certainty about what types of data would be subject to localization requirements. It could likely entail significant compliance costs and adjustments. Uncertainty at this stage strikes at businesses' ability to serve their Indian consumers freely and efficiently. ● The classification of CPD should be closely linked to the requirements of National Security. This will limit the impact of stringent localisation and offer certainty to businesses in their data processing activities. Seeking inspiration from the IT Act, which lays down the meaning of 'Critical Information Infrastructure' similar parameters should be given for CPD. We seek that the definitions of foundational terms such as PD, SPD, CPD and harm be harmonized with global regulations. If any unique additions are made to these definitions, we seek that they be clearly defined to ease compliance and regulatory certainty.
6.	**Expansion in the definition of "harm":** ● The JPC has extended the definition of "harm" under Section 3(23) of the DP Bill 2021 to include "psychological	**Issue:** ● The expanded scope of "harm" to include psychological manipulation creates ambiguity in the law.

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
	manipulation which impairs the autonomy of any individual", as well as enable the Central Government to prescribe other forms of harm.	**Comments:** ● We note that the rationale for expansion of the definition of "harm" is to account for new kinds of harm which may arise in the future due to technological innovations. However, since the phrase "psychological manipulation which impairs the autonomy of any individual" is undefined and unclear, it can impact several services provided by data fiduciaries, including targeted advertising services which assist local businesses in improving their reach, enable the consumers to find affordable products, etc. ● Therefore, the MEITY should reconsider the incorporation of this phrase under the definition of harm under the DP Bill 2021, especially because this is out of sync with global privacy laws. Alternatively, it should clarify its meaning.
7.	**Age of consent:** ● The DP Bill 2021, under Section 3(8), continues to define a "child" as a person under 18 years of age. The age of consent under Section 16 has, therefore, neither been reduced nor has a sliding scale been introduced for the ages of 13 to 18 years. By virtue of this, the obligation of data fiduciaries to verify the age of a child, as well as obtain consent from their parent/legal guardian in order to process their PD remains as is.	**Issue:** ● The law fails to recognise the varying levels of maturity of young persons who belong to different age groups and is not at par with the global standards on treatment of PD of young persons. **Comments:** ● We understand the necessity to obtain parental consent for children below 13 years of age in order to safeguard their interests. However, we believe that an exception should be made to enable the consumption of services by young persons between 13 to 18 years of age, who may be mature enough to make decisions about their PD and can also benefit from a variety of services on the internet. In fact, other laws, such as the GDPR, have permitted countries to fix digital age-gates ranging from 13 to 16 years, enabling

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		young persons who belong to this age group to make their own decisions about their PD. ● Further, we understand that there may be legitimate concerns like harmful use of minor's PD, etc. which makes parental consent necessary. However, even after consent is provided by a parent, misuse of data cannot be ruled out, and the other provisions in the law would serve to safeguard against this possibility. Businesses should also be able to process young person's PD for limited, pro-consumer and non-harmful purposes (for instance, to recommend online content – such as educational videos) without having to obtain parental consent. Moreover, requiring parental consent can sometimes work to the detriment of young persons and hinder access to important services, i.e., there may be instances where parents withhold consent to critical and essential online resources that young persons may need (such as counselling, suicide prevention, etc.). ● Businesses may also be face constraints in offering beneficial services to young users due to technological complexities involved vis-à-vis consent and age verification obligations. This is because, at the moment, it may not be technologically feasible for businesses to single out and determine which of their existing users are minor users, without verifying the age of all users. The costs associated with such widespread verification are extremely high and will also require collecting additional PD from users (in order to determine their age), consequently creating more privacy risks. ● Therefore, the current age-gating and verification requirements should be reconsidered by the MEITY. If age verification continues to be mandated, data fiduciaries should be allowed to develop their own mechanisms and should not be

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		required to follow mechanisms laid down by the DPA.
8.	**Prohibition on tracking, monitoring, etc.:** Since the concept of "guardian data fiduciary" (**GDF**) has been removed, now, under Section 16(4) of the DP Bill 2021, all data fiduciaries are barred from "profiling, tracking, or behavioural monitoring of, or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child".	**Issue:** ● The blanket prohibition under Section 16(4) can deter data fiduciaries from keeping their minor users safe online, creating personalised content in their interests, etc. **Comments:** ● We believe that this blanket prohibition should be reconsidered on two grounds: - Since data fiduciaries may not always know the age of all users, one possible method of knowing the same (especially in order to comply with their age verification obligations, if retained) would be to monitor user activity to determine the age group of a user. Such monitoring may also qualify as "profiling". However, since both monitoring and profiling are barred, data fiduciaries would be prevented from detecting underage users and treating them differently (as done by many companies and recommended by the JPC itself). - Further, the blanket prohibition on targeted advertising is based on the assumption that all targeted advertisements go against minors' interests. However, this is not always true as some data fiduciaries may wish to target content and advertisements to young persons for beneficial services relating to education and well-being. - Lastly, since tracking is also banned, it will become increasingly difficult for data fiduciaries to ensure online safety of minors, which they were earlier able to do so by keeping a track of their activities.

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		- In light of the above, we urge the MEITY to reconsider Section 16(4) of the DP Bill 2021. It should only prohibit those processing activities that cause significant harm.
9.	**Services to not be denied based on choice, etc.:** ● The JPC has amended Section 11(4) of the DP Bill 2021 to add a requirement, i.e., any service or good or performance of a contract, etc. cannot be denied to a data principal based on the exercise of choice.	**Issue:** ● The JPC Report nowhere clarifies the rationale behind and how this "choice" based amendment should be interpreted. **Comments:** ● In light of the ambiguities introduced by this proposed amendment, it is currently unclear what has to be done in cases where a service (such as an ed-tech service) simply cannot be provided by a data fiduciary without consent from a data principal to process their PD that is essential to provide such service (such as their grade/class). Further, "exercise of choice" is a broad term and if companies are required to continue to provide services upon any kind of exercise of choice, it will render the whole of Section 11 and the entire consent-taking process redundant. Accordingly, the MEITY should reconsider this amendment. ● Separately, we would like to bring the MEITY's attention to another aspect of Section 11(4) of the DP Bill 2021 which mandates that data fiduciaries should not deny services, etc. to a data principal merely on the basis of a lack of consent from such data principal provide PD that is not "necessary" for the relevant purposes. We note that no standard has been laid down to delineate what PD may be "necessary" to provide a service. In fact, the threshold for necessity would depend upon the exact nature of service being provided. For instance, a basic version of a service will require less PD as compared to a personalised version of the service. In light of this, a literal interpretation of Section 11(4)

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		suggests that a data fiduciary should always explain the necessity behind collecting a data principal's PD, at each level of collection and processing. A data fiduciary may also have to tweak its service for each data principal, based on the level of consent provided by a data principal. Such a scenario can lead to consent fatigue as well as impact the ease of doing business. Therefore, we urge the MEITY to provide clarity on this standard of "necessity".
10.	**Contractual necessity and legitimate interests as secondary processing grounds:** ● We note that the JPC has recognised legitimate interest as part of the "reasonable purposes" (as may be notified by the DPA) for processing PD without the data principal's consent under Section 14 of the DP Bill 2021. ● However, "contractual necessity" and "legitimate interests" as standalone and independent grounds for non-consensual process remain absent. ● The legal ground for processing SPD is also restricted to explicit consent.	**Issue:** ● Such requirements could be restrictive, and lead to disproportionate costs incurred by data fiduciaries in day-to-day operations. ● Data fiduciaries should be empowered to process PD without consent for both "legitimate interests" and "contractual necessity" upon making a self-determination of the need to carry out such processing – without the DPA's involvement. This will ensure parity with global standards. ● The DP Bill 2021 provides for 'reasonable purposes' as an alternate ground for processing in the absence of consent, the list of 'reasonable purposes' for processing of data under section 14(2) is highly restrictive and requires the DPA to notify the purposes. **Comments:** ● We note that the JPC has not accounted for industry and stakeholder requests to allow data fiduciaries to process PD and limited SPD on grounds of "legitimate interests" and "contractual necessity" without obtaining consent of data principals. ● Incorporation of these grounds will enable data fiduciaries to process PD to perform their

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		contractual obligations with data principals, without having to obtain duplicate consent for each instance of processing that is necessary to perform such obligations. Repeatedly obtaining consent from data principals can lead to consent fatigue. The reliance on consent for processing personal data in routine transactions where a requested service *cannot* be provided *without* processing personal data, may also trivialize the importance of consent, as the user would become accustomed to providing consent for all data collection activities. Similarly, data fiduciaries should be able to process PD and limited SPD without consent for their legitimate interests (to prevent fraud, ensure security of transactions, etc.). ● A ground should be available to the data fiduciary when processing data is necessary to deliver the data fiduciary's side of the contract with the data principal. The data required to enter into a contract or perform a contract must be within the scope of the contract and services offered. Reading this with the larger transparency obligation on data fiduciaries, would prevent any potential misuse and reduce burden on consent for every potential digital exchange between the consumer and the fiduciary. This ground is also recognised under the GDPR. ● <u>We urge the MeitY to consider the incorporation of contractual necessity (fulfilment of a contractual obligation) and legitimate interests as additional, non-consent based grounds of data processing to enable business continuity and ease of compliance, avoid consent fatigue of data principals and to place the DP Bill 2021 at par with global frameworks.</u> ● The DPA should come out with a code of practice for how an organisation should carry out

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		a self-determination exercise to determine 'reasonable purposes' for data processing and document the same as evidentiary proof. Such self-determination should take into consideration the rights of the data principles and carry out a balancing test.
11.	Overlapping rights: ● JPC has amended Section 20(1) of the DP Bill 2021 to now include even the right to prevent / restrict the processing of personal data, as part of the right to be forgotten.	**Issue**: ● The DP Bill 2021 under Section 20(1)(a) vests data principals with the right to restrict or prevent the continuing disclosure or processing of personal data, when such disclosure or processing has served the purpose for which it was collected, and is no longer necessary for the purpose. ● This is likely to lead to an enormous burden on the operations of the data fiduciary since personal data of a data principal may be linked to the data of other data principals, and also to underlying operations of the business. **Comments**: The additional right to restrict / prevent processing of the principal's personal data should be removed from the scope of the right to be forgotten and such right should be limited to continuing disclosures of the individual's personal data.
12.	Posthumous exercise of data principals' rights: ● The DP Bill 2021 introduces Section 17(4) that enables a data principal to nominate a legal heir / legal representative as a nominee to exercise the right to be forgotten and append the terms of the agreement with respect to the processing of personal data post the death of the data principal.	**Issue**: ● The manner in which the new provision has been drafted leaves significant room for interpretational ambiguity. **Comments**: The following points should be clarified in Section 17(4):

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		• Whether the rights vis-à-vis posthumous treatment of a data principal's personal data have to be exercised during the data principal's lifetime, or post the data principal's death? • Whether the phrase "appending the term of agreements" refers to amendment of agreements relating to the collection, processing and retention of a data principal's personal data? • What are the consequences of a data principal failing to explicitly nominate a legal heir or representative during their lifetime?
13.	**High civil penalties:** • Section 57 of the DP Bill continues to levy a penalty in case of certain contraventions between the range of 2 to 4% of the "total worldwide turnover" of a data fiduciary. However, now, the JPC has left the exact quantum of the penalty to be determined by the Central Government.	**Issue:** • The term "total worldwide turnover" is of wide amplitude and can lead to broad interpretation and heavy penalties being imposed. Further, the circumstances under which a penalty can be imposed are broad-based. **Comments:** • The term "total worldwide turnover" includes revenue generated by a data fiduciary outside India. However, such revenue may have no relation to the domestic processing activity on the basis of which a penalty may sought to be imposed. This also goes against the principle of "relevant turnover" recognised under other sectoral laws (such as the Competition Act, 2002 read with Excel Crop Care Ltd. v. CCI, (2017) 8 SCC 47, paragraph 91). • The Central Government also has wide discretion to prescribe the precise quantum of penalties that can range from 0.1 to 4% of the global turnover of a data fiduciary. Given that such high percentages can have significant consequences

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		for businesses, it will act as a disincentive to them to invest in India's tech sector. ● Further, the criteria for imposition of a penalty under Section 57 is expansive. For example, a penalty can be imposed on a data fiduciary if it fails to take "prompt and appropriate action in response to data security breach". However, there is a lack of clarity on what "prompt and appropriate action" entails. ● Lastly, under Section 65 of the DP Bill 2021, a data principal can seek personal compensation from a data fiduciary, even if a data fiduciary has faced penalties for the same contravention. This kind of double punishment should be avoided as it will undoubtedly affect the ease of business doing in India. ● In light of the above, we recommend the following safeguards be introduced in Section 57 of the DP Bill 2021: - Any penalty levied should not exceed the total gain/benefit/unfair advantage accrued to a data fiduciary due to a contravention. - A penalty should be based on an assessment of "significant harm" caused to any data principal - The term "total worldwide turnover" should be reconsidered. - Separately, the overlap in imposition of penalties and seeking of compensation should be addressed.
14.	**Disclosure of algorithmic transparency:** ● Section 23 of the DP Bill 2021 imposes extensive transparency requirements on data fiduciaries. However, the JPC has introduced an additional requirement of	**Issue:** ● The requirement of algorithmic disclosures raises intellectual property concerns for data fiduciaries.

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
	data fiduciaries disclosing the "fairness of algorithm or method used for processing of personal data". The rationale behind this inclusion is to prevent "misuse" of algorithms used to process PD.	**Comments:** ● We appreciate the positive goal of the JPC to safeguard the interests of data principals. However, we note that such disclosure may entail revealing their source code, algorithms, machine learning techniques, etc. This is especially because there are no safeguards under this provision to protect proprietary rights. ● Further, fairness of PD processing is already ensured through Section 5 and the definition of "harm" (which includes discriminatory treatment). These provisions will safeguard users from discriminatory or unfair treatment that may arise due to automated data processing activities. Data principles also have the option of claiming compensation under Section 65 in case of unfair processing activities. ● In light of the above, this addition should be reconsidered by the MEITY.
15.	**Transition periods under the DP Bill 2021:** ● The JPC, in the main text of the Report, recommends that an approximate period of 24 months be provided from the date of notification for implementation of all provisions of the DP Bill 2021.	**Issue:** ● Despite recommending transition provisions, JPC leaves the exact timelines to be decided by the Central Government. **Comments:** ● We urge the MEITY to provide transition periods within the text of the law. This will be in the interests of ease of doing business as it will provide certainty about the date from which the obligations under the DP Bill 2021 will become applicable (as was done under the GDPR) and will also ensure that companies have sufficient time to comply.
13.	**PDPB to cover Hardware Manufacturers**	● This recommendation appears misplaced, in as much as the PDPB's provisions are largely

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
	The JPC has commented on the lack of provisions in the PDPB that specifically address data collected by hardware manufactures through digital devices. In the Report, the JPC has repeatedly stressed on the need to regulate such data collected through digital devices. *Proposed Changes*: Central Government must establish a mechanism for the formal certification process for all digital and IOT devices to ensure the integrity of all such devices with respect to data security. In such context, the DPA may provide data security standards that would be enforced by the DPA and appropriate testing facilities be made available by the government. This would ensure the integrity and trustworthiness of such devices and prevent any malicious insertion in such devices which may cause breach of Indian data. The JPC further recommends including the manner of monitoring, testing and certification of such devices within the scope of the PDPB.	technology/industry agnostic. In any event, the intent of the JPC to increase the scrutiny and compliance burden on hardware manufacturers and importers is clear. ● As with some of the other provisions which unjustifiably expand the scope of this legislation, regulation of digital devices through the PDPB would change the pith and substance of the law from one on privacy and data protection, to one that is focused on digital regulation. As mentioned above the purpose of the PDPB is to protect informational privacy of individuals and the DPA constituted under it is to be a watchdog for individual privacy therefore shifting the focus the DPA to monitoring, testing and certification of hardware device would deviate from the intent of the legislation and may even question the constitutional validity of the PDPB. ● Even if such regulation is sought to be brought about, it is best done through other avenues, instead of muddying the objectives that the data protection law (grounded in enabling individual privacy rights) seeks to achieve. In fact, steps have already been taken in such a direction though the National Security Directive on Telecommunication Sector, whereby TSPs are mandatorily required to connecting their networks only those new devices which are designated as 'Trusted Products' from 'Trusted Sources'. Hence, such 'device regulation' should be kept out of the personal data protection legislation. There is already an existing regime for hardware certification in relation to devices sold in India. Multiple certifications sought under the existing regime, which fall under multiple regulators/ departments, such as TEC, WPC, BIS, Ministry of Electronics and Information

#	Report recommendation / text of DP Bill 2021	AIC's issues and comments
		Technology, etc. Involving the DPA as an additional regulator can result in uncertainty and confusion for the stakeholders and create conflict between different regulators. We do not see a need to introduce a separate certification process for devices only from a privacy and security point of view, since most entities already ensure that such devices are compliant with global standards from a privacy perspective. ● Moreover, data fiduciaries under the PDP Bill collecting personal or sensitive personal data of data principals are already subjected to a comprehensive regime under the PDP Bill, which includes obligations and safeguards in relation to how such data must be collected, processed, stored, etc. These obligations will continue to apply to hardware manufacturers who qualify as data fiduciaries under the PDP Bill. Given this, hardware certification for digital devices, which was never a part of discussions for the scope of the PDP Bill (provisions in the PDP Bill are agnostic of industry and technology), must be kept outside the ambit of the PDP Bill.