The Dialogue™
INFORM ENGAGE IDEATE

Response

NATIONAL HEALTH AUTHORITY'S DRAFT DATA SHARING GUIDELINES

Authors
Eshani Vaidya and Sreyan Chatterjee

ABOUT THE DIALOGUE

The Dialogue™ is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ was ranked amongst the Top-Ten think-tanks in the world to watch out for by the Think-Tank Civil Societies Programme, Lauder Institute, University of Pennsylvania, in their 2020 and 2021 ranking index.

 info@thedialogue.co

 www.thedialogue.co

INTRODUCTION

The National Health Authority ('**NHA**') has developed Data Sharing Guidelines to regulate the use of personal data of beneficiaries of the PM-JAY scheme. As highlighted in the guidelines, the scope of application extends to data across the digital health ecosystem that includes PM-JAY as well as Health Wellness Centres and the ecosystem partners. It is important to note that data management within the digital health ecosystem also includes the Health Data Management Policy, and the outward policies governing the use and sharing of non-personal and personal data.[1]

At the outset, The Dialogue™ would like to commend the National Health Authority for their approach towards enabling data management and smooth data flows across the digital health ecosystem. The guidelines, while comprehensive, require further clarity on a few aspects, such as the approach towards secondary use of data, the role of the NHA as a data fiduciary and the manner in which sensitive personal data will be protected.

The Dialogue™ discusses the aforementioned aspects thematically, in the following order—data protection, cyber security, governance and community. Our findings and recommendations have been buttressed by our work in digital health in the past, including our report titled 'India's Digital Health Dreams: Getting it Right'. Our recommendations are more focused on ensuring the principles of data protection and sharing that have been delineated are effectively operationalised. Therefore, we suggest ways in which the provisions can be further strengthened to enable smoother flows of data within the PM-JAY.

[1]Such as the National Data Governance Framework Policy, draft Personal Data Protection Bill, 2019, the NPD Framework etc.

ASSESSMENT FRAMEWORK

Our work spanning India's digital health initiative culminated in the publication of our report titled 'India's Digital Health Dreams: Getting it Right'. Within this Report, we developed an assessment framework in an attempt to capture the flux of law and policy in digital healthcare.[2] We assessed policy requirements at the level of legislation, policy, and the implementation of operational best practices. We suggested a model list of questions that may be used to assess a government digital healthcare system, a policy framework, or a digital healthcare provider.

It is against this assessment framework that we have evaluated the Data Sharing Guidelines under the PM-JAY scheme. We have extracted the relevant portions of the assessment framework in order to add nuance to the conversations around digital health, temper expectations and focus on the essential prerequisites for successful interventions under the PM-JAY.

[2] S. Chatterjee, K. Venkatesh, E. Vaidya (2022) India's Digital Health Dreams: Getting it Right, The Dialogue.

Question	Provisions in Guidelines	Assessment	Recommendations
Data Protection			
Is there a national data protection law in place?	N/A	At the moment, there is no legislation for data protection. However, the Personal Data Protection Bill, 2019 was referred to the Joint Parliamentary Committee ('**JPC**') in 2019. Following its fifth extension, the JPC tabled its report on the Bill in the Parliament's Winter Session of 2021.[3] Protection of personal data and sensitive data is currently covered under the Information Technology Act and the 'SPDI Rules'.[4] There remains significant scope to increase data protection at scale.	In the absence of a data protection law, policies must provide for the following: – High technical standards (such as standards of anonymisation and interoperability) should be developed in collaboration with the relevant stakeholders. – We must clarify the manner of enforcing penalty for compliance under Cl.12 work in the absence of a data protection law, considering the inadequate provisions of the IT Act and related Rules for the same. – In addition to the institutionalisation of audit trails, 'social audits' must also be institutionalised. The primary difference between the two is that social audits mandate a bottom-up approach and institutionalise a form of community engagement.[5]
Are data sharing agreements effectively regulated?	Cl. 9.1.3 assigns the NHA Data Sharing Officer ('**DSO**') responsibility for regulating contracts, including service-level agreements. Cl. 9.6.2. provides that requests for access to personal data must be approved by the Data Sharing Committee ('DSC'). It further states that the decision of the DSC will be final and 'there shall be no provision of appeal'.	In essence, these are the provisions of a 'data sharing agreement'. It is within this agreement that the rights of data principals are guaranteed in direct relation to the data fiduciaries.	Data sharing agreements must be made public and must set out the entire lifecycle of data.[6] This is particularly important when contracts with third-party vendors are entered into because the end-use of data is not always visible.[7] Specify how such data (i.e., shared data) will be monetised.[8] Mandate periodic participatory meetings with beneficiaries, end-users in order to review policies and make case-by-case decisions where necessary.[9]

[3] Principles 5 and 6, Cl. 7, Data Sharing Guidelines, National Health Authority.
[4] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
[5] S. Chatterjee, K. Venkatesh, E. Vaidya (2022) India's Digital Health Dreams: Getting it Right, The Dialogue.
[6] S. Chatterjee, K. Venkatesh, E. Vaidya (2022) India's Digital Health Dreams: Getting it Right, The Dialogue.
[7] S. Chatterjee, K. Venkatesh, E. Vaidya (2022) India's Digital Health Dreams: Getting it Right, The Dialogue.
[9] S. Chatterjee, K. Venkatesh, E. Vaidya (2022) India's Digital Health Dreams: Getting it Right, The Dialogue.
[9] S. Chatterjee, K. Venkatesh, E. Vaidya (2022) India's Digital Health Dreams: Getting it Right, The Dialogue.

Question	Provisions in Guidelines	Assessment	Recommendations
	Cl. 9.6.7. provides for contracts signed with vendors in the context of anonymised data. Cl. 9.7.6. provides for the responsibility of ecosystem partners to comply with security safeguards as 'per contractual duties'.		– The DSCs response to a data sharing request must have a provision of appeal so as to prevent exclusionary harms. The escalation mechanism can open up access to the Data Protection Authority under the draft Personal Data Protection Bill, 2019 ('**PDP Bill**') and further the relevant Ministry. – Model contract clauses that lay down liability on third party vendors should be shared publicly in a way that does not endanger the privacy of the vendor or of the governmental agency.
Do the guidelines provide for principles based on which data-related practices will be carried out?	Cl.8 provides for the principles of accountability, openness/transparency, privacy by design, collection limitation, purpose limitation, empowerment of beneficiaries, minimum and necessary uses and disclosures and security safeguards.	Principles must be a stepping-stone towards expressly defining the contours within which data sharing activities can take place. These will lay the groundwork for enforcement and maintenance of data-related rights of the data principal. In the absence of legislation, however, the principles of accountability and transparency, among others, are unlikely to have the desired effect.	– Openness and transparency are not synonymous terms. In addition to making several documents public, the guidelines must also provide for the manner in which beneficiaries will be able to meaningfully exercise their agency. The 'freedom to participate'[10] must be guaranteed under legislation and falling short of that under these guidelines. – A first step towards building accountable practices is to expressly provide for data-related rights and its corresponding duties. Following the assignment of liability, the oversight and enforcement mechanisms (social audits for instance) can be built. – Reasonable security safeguards must clearly provide for— • who determines 'reasonability'; • how such checks will take place; and • a consultative process (a continuous feedback mechanism) in place for the same.
Does the law clearly define the kinds of data that will be collected?	Cl. 6 of the Guidelines provide for 'type of personal and sensitive personal data collected'. It is important to note that 'purpose limitation' has been highlighted under	The principle of 'purpose limitation' requires the draft and enforcement of specific and actionable provisions. However, without such provisions being	– Cl. 9.6.5. must be extended to include: – Data that can/cannot be processed. – The manner in which such 'purpose' will be evaluated.

[10] Critical Perspectives of Open Development: Empirical Interrogation of Theory Construction, pg 5.

Question	Provisions in Guidelines	Assessment	Recommendations
	under the Guidelines. Cl. 9.6.5. delineates the purposes for which only anonymised or de-identified data can be used. Cl. 9.8.2. prevents use of health data under these Guidelines for commercial purposes.	expressly delineated, it is likely that enforcemet will be challenging. In order to study the manner in which management of anonymised and de-identified datasets one must analyse not only the restrictions or limitations imposed, but further the manner in which these limitations are enforced. Express provisions i.e., devoid of ambiguity are an essential part of ensuring that the data principal's rights are adequately protected.	– The manner in which it shall be highlighted in the privacy policy. – Phrases like 'reasonable efforts to use (...) only the minimum amount of personal data' must be clarified. What these 'reasonable efforts' would include must be clearly laid down. – Define 'commercial purpose'[11] to prevent misuse of health data appropriately and effectively. – The permissioned use of health data for 'secondary use' such as research, innovation and other legally valid activities must be clearly laid down. Similarly, the prohibition of use of health data for commercial purposes must be clearly provided, such as the use at the cost of the data principal's interest. – The restrictions must be feasible and must not conflict with other data sharing policies and guidelines in place. Cl. 9.6.5.(e) must clarify the scope of 'related purposes'. – Under cl. 9.5.1.(a)(b) information made public regarding processing activities must also include the purpose for which the third party has accessed the data. A list that is updated at regular intervals must contain details of the names and purpose. Such a dashboard can provide a quick look at change in purpose as well (if it reflects real time updates).
Are there privacy by design systems that minimise the harms from a data breach?	Cl. 7 Principle 4 provides for Privacy by Design. It is meant to 'anticipate, identify and avoid harm to the data principal'.	Privacy by design systems use best practices on data protection, with failsafes, backups, and appropriate security. Instead of putting the onus on administrative competence, they	– NHA must publish the relevant enforcement policy in consultation with experts, especially considering the absence of a data protection legislation. – The policy must mandate disclosure of breaches to the user and relevant stakeholders.

[11] Annexure-I, Data Sharing Guidelines, National Health Authority.

Question	Provisions in Guidelines	Assessment	Recommendations
		create relatively fool proof systems that do minimise data collection, limit purpose and access, and ensure that there are proper safeguards against unauthorised use.	– Ensure privacy-by-design audits of the system prior to roll-out.
Have the risks related to anonymisation of data been considered?	Cl. 9.10.6 provides that the anonymisation of data shall be done by NHA in accordance with technical processes and anonymisation protocols that may be specified by the NHA. Cl.14(c) defines anonymisation as an 'irreversible' process.	Anonymisation cannot be truly irreversible.[12] Studies have shown that risks to individual privacy are not entirely abated even with anonymised data.[13]	– Anonymisation must be treated as a necessary 'first step' towards data protection but cannot be the only approach towards securing individuals personal data. – Anonymisation procedures must be in compliance with international standards and must be determined after consulting experts. – Distinction between anonymised and de-identified data must be expressly laid down.[14]
Are policies regarding best practices in the collection, use, and retention of sensitive data laid down?	Cl. 9.12 provides for data retention and disposal. The erasure of data can and will take place only upon the fulfilment of certain conditions. Cl. 5 provides mechanisms for collection of personal data and 9.2 provides for the privacy notice for collection or processing of personal data.	– Privacy notice to be submitted prior to the collection is a good move. – While implementing PM-JAY these aspects must be laid down, policies must be standardised and redlines must be clearly demarcated. For example, secondary use of data must happen within a defined framework that respects rights and user agency.	– Define primary and secondary uses of data at the time of consent collection. Cl. 9.4.2. must also provide for the use of health data in life-threatening instances, where the data principal cannot give consent. Exceptional disclosures must be appropriately demarcated. – Cl. 9.2.1. (b) should clarify that consent must also be obtained in case of a modification of purpose. This will come under a 'previously unidentified purpose'. – A separate policy[15] must determine the secondary use of health data for statistical, research, and development purposes.

[12] Amber Sinha et.al., Comments and Recommendations to the Personal Data Protection Bill, 2019, https://cis-india.org/accessibility/blog/cis-comments-pdp-bill-2019.
[13] Amber Sinha et.al., Comments and Recommendations to the Personal Data Protection Bill, 2019, https://cis-india.org/accessibility/blog/cis-comments-pdp-bill-2019.
[14] Cl. 9.8.2, Data Sharing Guidelines, National Health Authority.
[15] Government of Finland (Ministry of Social Affairs and Health), Secondary use of health and social data, https://stm.fi/en/secondary-useof-health-and-social-data.
[16] Regulation of the European Parliament and of the Council On the European Health Data Space, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197&from=EN.

Question	Provisions in Guidelines	Assessment	Recommendations
		– In case of withdrawal of consent, the 'legal consequences of such withdrawal' as provided under cl. 9.4.2.1. must not be borne by the beneficiaries. This will have a stifling effect on free consent.	– This must be accompanied by a 'data quality and utility label[16] that will allow third parties to identify datasets best suited to their use. – Cl. 9.3.2. (d) should be modified to mandate the disclosure of third-party details such as name and purpose for data collection. In case of a restriction due to conflict with IPR or other economic rights, the rationale behind withholding information must be provided to the data principal in writing. – The disposal of personal data must be accompanied by a mechanism to provide a certificate of such disposal to the concerned beneficiary.
Are the data related rights of beneficiaries expressly granted?	Cl 8., Principle 7 provides for the 'empowerment of beneficiaries'. Cl. 9.5.2. provides that beneficiaries must bear the cost, if any, of exercising their rights to confirmation, access, restricting disclosure among others mentioned under cl. 9.5.	In order to exercise meaningful agency over their data, the rights of data principals must be expressly laid down. The cost of exercising such rights must not be borne by beneficiaries as it is likely to deter exercise of agency.	– The principles of data sharing in cl.8 must include data rights, including economic rights. – A mechanism to provide for the rights of minors as data principles must be developed, including the opportunity to be opt-out once the minor attains the age of majority. This is in line with the recommendations laid down by the Hon'ble Supreme Court in the case of Justice K.S. Puttaswamy v. Union of India[17] and the legislative backing of the Aadhaar Act, 2016. – The role of 3rd party privacy technology consent management vendors for beneficiaries under PM-JAY must be clarified. – Cl. 9.3.2 should be amended to include--'specify the rights granted to each data principal i.e., beneficiary under this scheme, including but not limited to the right to be forgotten. – As an alternative to a user fee to access data rights, tax funded approaches must be explored.

[17] (2017) 10 SCC 1.

Question	Provisions in Guidelines	Assessment	Recommendations
Is there a common standard for graded datasets, based on a risk assessment laid down in the policy framework?	Cl.9.1.3. (d) the NHA DSO must maintain a data sharing risk register that will be periodically reviewed by the NHA.	In the adoption of a holistic approach towards cybersecurity, and maintaining proportionate compliance standards, it is important to develop a mechanism to grade data sets. This will allow specific regulation of data sharing of data sets in accordance with the risk-level determined. It will also benefit MSMEs, as their compliance obligations will be proportionate to that of the risk associated with their datasets.	– Classify data based on its nature and the risk associated with it. For example: anonymised, non-person or personal data or operational information distinct from personal health records. – Conduct risk assessments to identify sensitive categories and define acceptable data practices for each classification. – On the basis of such classification, set bright lines for use, storage and sharing of data. – Show citizens the source, nature of data, and conditions for making datasets available.[18] – A dataset information sheet must be developed that will contain relevant details such as the manner of classifications of datasets, the associated levels of security, and who has access to their data and for what purpose. This must include private and government agencies alike.
Is there a detailed manual for stakeholders to sensitise to best practices in data, such as how to grade data at source?	Annex-I provides for sensitisation and training of personnel dealing with sensitive personal data and personal data. Cl. 9.13 provides for training and awareness. These are to be conducted by the NHA.	Training is restricted to maintaining the 'need to know' status quo. While these measures are wholly inadequate, a more noteworthy absence is that of skill-based training. This is important to ensure that accurate datasets are maintained across the ecosystem.	– Enforce performance standards for data sharing practices across its various forms. – Training programmes must also extend to the private actors that are a part of this ecosystem. – In addition to general behavioural sensitisation, it must also include: • The manner of data collection and entry; and • The identification and rectification of invalid entries etc.

[18] Regulation of the European Parliament and of the Council on the European Health Data Space, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0197&from=EN.

Question	Provisions in Guidelines	Assessment	Recommendations
Cybersecurity			
Is there a mitigation strategy in place in case of failure or coordinated attack on the data systems?	Cl. 9.11 provides for Data Breach or Incident Management. This includes the mandate of reporting breach-related incidents to the Data Sharing Committee. This Committee will also be granted the power to 'take action under law (...) in relation to such breach as it may deem fit.' [19] Cl. 9.11.7. mandates 'timely notification of breaches' by the NHA ecosystem partners.	The Data Sharing Committee is not a judicial body. It has not been granted 'quasi-judicial' powers by legislation either. Therefore, it cannot be the final arbiter of disputes regarding 'data breaches and incidents management'. This would violate one's fundamental right to access justice under Article 14 and 21 of the Constitution of India.	– Develop a healthcare big data security monitoring and early warning system for breaches.[20] – Build capabilities and specific defences against cyber espionage to protect intellectual property.[21]: – Conduct period risk assessments of the cybersecurity system as whole in order to identify shortcomings and improve security mechanisms.[22] – Certification and labelling schemes can be adopted across the ecosystem to increase citizen trust in services.[23] – Replicate existing institutions such as the Indian Computer Emergency Response Team ('**CERT**') (National and State level) to operate within the health sector.[24] – 'Timely notification' as a mandate is vague. The ambiguity may lead to poor reporting hygiene. Therefore, timelines must be laid down so as to improve accountability within the ecosystem. – Use data acquired through audit trails to identify areas of concern and strengthen the same.[25] – Standardise practices (in a graded manner, where obligations for primary healthcare centres are different from large private hospitals)[26]

[19] Cl. 9.11.2, Data Sharing Guidelines, National Health Authority.
[20] Rule 19, Meghalaya Social Audit Rules, 2019.
[21] Rule 20(12), Meghalaya Social Audit Rules, 2019.
[21] Article 78 of the GDPR provides for the "right to an effective judicial remedy against a supervisory authority"
[22] National Health Service, How to complain to the NHS, https://www.nhs.uk/using-the-nhs/about-the-nhs/how-tocomplain-to-the-nhs/.
[24] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5,2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.
[25] Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data (DataInsider, Sep. 17, 2020), https://digitalguardian.com/blog/ healthcare-cybersecurity-tips-securing-private-health-data.
[26] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

Question	Provisions in Guidelines	Assessment	Recommendations
In the effort to improve cyber hygiene, have any investments been made in information sharing?	9.11.2. Cybersecurity incidents are to be reported to the Data Sharing Committee.	A holistic approach towards cybersecurity management involves an *ex-ante* approach. In order to successfully operationalise the same, we need to develop standards for reporting that will 'bridge the knowledge gap'. For instance, CERT have issued 'security tips for common users' that can be accessed on their website.[27]	– Take initiative to improve awareness of available assistance initiatives (victim support, training, and certificate courses that healthcare providers can undertake etc.)[28] – Invest in cyber hygiene training and certificate courses to educate healthcare staff.[29] – Train cybersecurity professionals to deal with the unique challenges/risks associated with healthcare, including increased familiarity with medical technology.[30]

[27] Ministry of Electronics and Information Technology, Indian Computer Emergency Response Team, https://certin.org.in/.
[28] The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People (2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.
[29] Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data (DataInsider, Sep. 17, 2020), https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data.
[30] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co- Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

Question	Provisions in Guidelines	Assessment	Recommendations
Governance			
In line with the principles of accountability and transparency, have the relevant aspects of governance of the Data Sharing Committee been highlighted?	Cl. 9.1. provides for the constitution of a Data Sharing Committee with three members.	Considering the fact that the DSC is going to have significant control over the data flows of the digital health ecosystem, expressly providing for its scope and limitations is important to avoid arbitrary action.	– Provide for the constitution of the body i.e., its members and their tenure. – Similarly, the operations of the to-be established Privacy Operation Centre under cl. 9.1.2. must be clearly delineated.
Has the role of the NHA as a data fiduciary been clarified?	Several provisions across the guidelines provide for the duties of the NHA as a data fiduciary. For instance, cl. 9.2.1. states that 'NHA as data fiduciary shall give a clear and conspicuous Privacy Notice' to the data principals.	With the PM-JAY being governed by the NHA and the NHA developing guidelines for data sharing, it is unclear how its relationship with other entities such as the Data Sharing Committee will be overseen. Additionally, the obligations of data fiduciaries within the ecosystem have also been confused with those of 'actors in the ecosystem', which may unwittingly create loopholes.	The following aspects need further clarity: – Do the obligations of the NHA as a fiduciary extend to all data fiduciaries? – Are data fiduciaries and 'ecosystem partners' being used as synonymous terms? This is an important clarification because the obligations and liability associated with data fiduciaries is vastly different from that of any ecosystem

Question	Provisions in Guidelines	Assessment	Recommendations
Community			
Are there effective civil and criminal redressal mechanisms in place to deal with violations of their rights arising from the use of data?	Cl. 10 provides for grievances and complaints redressal. If the complaint cannot be adequately handled by the NHA, complainants may approach the MoHFW.	Access details to the call centre/postal address cannot be found. Therefore, it remains inaccessible to several groups.	Information Sharing – Posters (put up across hospitals) and other IEC channels should ensure that the grievance redressal hotline number and the URL of the website are prominently published. – Provide information regarding the first point of contact (preferably at the community level, such as ASHA workers). Redressal Process – Allow for phone-based complaint registration through IVR system as well as call centre. Additionally, both phone-based processes and the website should be accessible in local languages. – Timeline for acknowledgement of complaint must be clarified. – Provide adequate escalation mechanisms to a judicial or quasi-judicial body with power to direct the NHA, DPA under the PDP and other relevant bodies.[31] Resolution – The aggrieved party must have access to the status of resolution i.e., action taken. – Collection of complaint handling data can be used to identify areas of improvement within healthcare providers.[32]
Are there suitable alternatives to Aadhaar as a foundational identifier so as to create an inclusive system?	Cl. 6 provides for the type of personal and sensitive personal data collected by the NHA and its ecosystem partners. Subclause (b) provides for the documents that can be furnished as proof of address.	It is important to allow multiple government-issued identification documents to be used in place of Aadhaar so as to ensure that the PM-JAY scheme covers a more inclusive array of beneficiaries.	– The data collected under Cl.6 must appropriately distinguish personal and sensitive personal data. Treating the two as the same through a broad-strokes approach may lead to privacy-related harms – Clarify that for proof of address any of the documents mentioned in cl.6 (b) can be used to enforce inclusive processes.

[31] Article 78 of the GDPR provides for the "right to an effective judicial remedy against a supervisory authority".
[32] National Health Service, how to complain to the NHS, https://www.nhs.uk/using-the-nhs/about-the-nhs/how-tocomplain-to-the-nhs/. Act, 2017, p. 16, https://safar-india.org/documents/PILOT%20SOCIAL%20AUDITS.pdf.

Question	Provisions in Guidelines	Assessment	Recommendations
Are exclusionary harms arising from automated processing of data adequately addressed?	Cl. 9.5.1. (d) provides that a user can object to, and not to be subject to a decision based solely on, automated processing (including profiling), which produces legal effects or significant effects on the data principal.	Only allowing objections on decisions based solely on automated processing will create dangerous loopholes within the accountability mechanism in the ecosystem.	– Amend 'solely' to 'majorly' to read: 'Object to, and not to be subject to a decision based majorly on, automated processing (including profiling), which produces legal effects or significant effects on the data principal.'

The Dialogue™

INFORM ENGAGE IDEATE

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The DialogueTM has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

https://thedialogue.co