JINDAL SCHOOL OF BANKING & FINANCE
India's First Global Finance School
JINDAL GLOBAL UNIVERSITY

O.P. JINDAL GLOBAL
Institution of Eminence Deemed to be
UNIVERSITY
A Private University Promoting Public Service

RESPONSE TO DRAFT DATA CENTRE POLICY, 2020

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY

NOVEMBER, 2020

Shohini Sengupta, Keerti Pendyal, Ashaawari Datta Chaudhuri

About the Authors

This submission is drafted by Shohini Sengupta, Keerti Pendyal and Ashaawari Datta Chaudhuri in response to the draft Data Centre Policy prepared by the Government of India's Ministry of Electronics & Information Technology.

Shohini is an Assistant Professor of Research with the Jindal School of Banking and Finance at the O.P. Jindal Global University, Sonepat, Haryana. She has a degree in law from the National Law Institute University, Bhopal and a MSc in Law and Finance from the University of Oxford. She teaches courses on technology law and financial regulation.

Keerti is a Lecturer with the Jindal School of Banking and Finance at O.P.Jindal Global University, Sonepat, Haryana. He is pursuing his PhD in Public Policy and Management from IIM Calcutta and has a PGDM from IIM Ahmedabad. His areas of research are technology laws and intellectual property laws.

Ashaawari is an Assistant Lecturer with the Jindal School of Banking and Finance at O.P.Jindal Global University, Sonepat, Haryana. She holds a degree from School of Law, KIIT University and an LLM in Intellectual Property Rights and Technology law from the National University of Singapore (NUS). Her areas of research are technology laws, intellectual property rights and banking and finance laws.

The authors are grateful to Professor (Dr.) Ashish Bharadwaj, Professor and Dean of the Jindal School of Banking and Finance for his guidance.

The views of the author are personal, and do not reflect any institutional opinion. All errors are attributable to the authors alone.

The authors can be contacted at shohini@jgu.edu.in, kpendyal@jgu.edu.in and adchaudhuri@jgu.edu.in respectively.

TABLE OF CONTENTS

RESPONSE TO THE DRAFT DATA CENTRE POLICY, 2020

OVERVIEW

The authors would like to thank the Ministry of Electronics & Information Technology (MeitY) for giving them the opportunity to respond to the draft Data Centre Policy, 2020 (Policy). We appreciate MeitY's endeavour to seek comments on the draft policy and clarify the policy position on the establishment of data centres in India.

However, after an analysis of the extant Policy, we believe that the Policy could benefit from a few changes recommended in the brief below. We believe that for a robust functioning of a modern data economy in India, it is paramount that a policy governing data centres is holistic in its conception and implementation. To this extent, we have made certain suggestions on the definitions, regulatory, environmental and other standards, along with some prerequisite observations at relevant places.

The comments and suggestions have been made in two parts in this document. The broad thematic areas on which the recommendations are based are: *definitions, data localisation* and *digital sovereignty, technical standards,* and *regulatory architecture*.

'Part A' presents an executive summary of all the recommendations. **'Part B'** delves into a more thematic and detailed discussion on the broader principles of the suggest reforms and international best practice.

PART A
EXECUTIVE SUMMARY

Clause No.	Topics	Comments
1.3	**Definition of Data Centre**	It is recommended that the definition of data centre is revised to include different classifications of such centres, and also allude to the critical functions carried out by them, including all building, equipment and power resources that help in processing of data.
1.4	**Emphasis on data localisation and digital sovereignty**	Extant Policy is recommended to be framed within the context of a wider data protection law, which details the various protections and safeguards available to users, and strengthens consumer protection and trust. The mandate of data localisation is recommended to be reconsidered on account of a number of economic, social, and regulatory burdens it will place on small businesses and the users at large. It is also recommended that an impact assessment is carried out before implementing the Policy. Further, the focus of digital sovereignty in the Policy through data localisation should be realigned to focus on the autonomy of people. To better address the question of digital sovereignty, alternatives such as the adoption of the free software principles be considered.
5.1.3.2	**Setting up of Pre-provisioned Data Centre Parks**	It is recommended that the status and quality of the power infrastructure in the country is improved to support data centres. There is also a requirement to improve the supply of water resources and streamline the mechanisms for resolving water disputes between states. Further it is recommended that an environmental impact assessment is made a

		regulatory requirement for data centres to measure the impact on carbon footprint and the environment.
5.1.5.2	**Incentives for domestic IT hardware including servers, storage, network devices, etc. and non-IT equipment such as mechanical, electrical, plumbing, cooling equipment etc**	It is recommended that since setting up chip fabrication plants is a very investment heavy activity, laws protecting intellectual property rights (IPR) and enabling efficient resolution of disputes be strengthened to increase trust and attract investments. Therefore, there is a requirement to improve IPR protection, speeding up dispute resolution including strengthening mechanisms of alternate dispute resolution.
5.4.1.1	**Promoting and encouraging the use of indigenous hardware.**	
5.2	**Standards and specifications**	It is recommended that MeitY consider adopting global best standards to attract investment, while tailoring them to suit the particular requirements of India and for shaping future standards in the subcontinent. It is proposed that this is done in collaboration with various stakeholders, including the Government, companies, and academic institutions from various disciplines including engineering, law, policy and management.
5.4.4	**Promoting the adoption of established global standards.**	
5.5	**Institutional Mechanism for policy governance**	It is recommended that instead of the Inter-Ministerial Empowered Committee (IMEC) and the proposed Data Centre Facilitation Unit (DCFU) the Government consider making the proposed Data Protection Authority (DPA) under the proposed Draft Personal Data Protection Bill, 2018 the nodal agency to regulate and co-ordinate all data centric policy implementation. The IMEC and DCFU can also seek to assist the DPA in carrying out its functions. Further, the IMEC, DCFU and the Data Centre Industry Council can act as a supplemental forum of policy governance, to support the primary regulatory functions

		undertaken by the DPA, with due consultation from other relevant Government bodies and ministries, and relevant state governments.

\

PART B

I. DEFINITIONS

Definition of data centre to be revised: Data centre in the Policy ('table of definitions') has been defined as "a dedicated secure space within a building / centralized location where computing and networking equipment is concentrated for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of data."

In this regard, the European Code of Conduct on Data Centers Energy Efficiency[1] defines data centres as including "all buildings, facilities and rooms which contain enterprise servers, server communication equipment, cooling equipment and power equipment, and provide some form of data service". This includes the large scale mission critical facilities and the small server rooms located in office buildings. Similarly, the United States (U.S.) Environmental Protection Agency (EPA) defines data centers as "facilities that primarily contain electronic equipment used for data processing (servers), data storage (storage equipment), and communication (network equipment)".[2]

Given that the policy covers all kinds of data centres in India, it is proposed that the definition is revised to include different classifications of such centres, and also allude to the critical functions carried out by them, including all building, equipment and power resources that help in processing of data.

[1] Code of Conduct on Data Centres Energy Efficiency – Version 1.0, 30 October 2008, European Commission Directorate-General Joint Research Centre

[2] Report to Congress on Server and Data Centre Energy Efficiency – Public Law109-431, U.S Environmental Protection Agency, ENERGY STAR Program, August 2, 2007

II. DATA LOCALISATION AND DIGITAL SOVEREIGNTY

A. Data localisation

In clause 1.4, the Policy outlines the need for data localisation. As per the Policy, this emphasis on data localisation stems from a draft law – the proposed draft Personal Data Protection Bill, 2018 (PDP Bill) still under Parliamentary consideration. It is proposed that MeitY re-consider the data localisation mandate on account of a number of economic, social, and regulatory burdens it will place on small businesses, users and the Internet ecosystem in India.

(i) Restrictive Impact on Interoperability and Data Economy: It must be noted that the principle of data localisation has been criticised by the United Nations (UN) for presenting significant barriers to all businesses, but in particular for being challenging for smaller businesses and new entrants by negatively affectin interoperability.[3] The UN report also stressed that instead of ensuring privacy or data security, localisation in fact creates a host of targets for hackers.[4] Further, it allows for a more expensive and inefficient alternative to flexible and compatible privacy regimes. The report also highlighted the onerous economic burden that localisation mandates place on small businesses, affecting a wider market than just Internet companies. As such, these policies are likely to hinder broader economic development, rather than promote domestic industry. To this extent, economists at the European Centre for International Political Economy (ECIPE) have found that data localisation could have significant negative domestic economic effects on the countries that choose to adopt such regimes.[5]

Further, data localisation regimes have been criticised for placing restrictive burdens on the Internet ecosystem, apart from also potentially violating trade obligations when applied indiscriminately.[6] Such restrictive policy mandates may also have an adverse impact on effective cross-border flows of data, essential to the operation of most Internet companies and e-commerce websites. Therefore, this would restrict effectual interoperability.[7]

(ii) Negative Impact on Economy and absence of impact assessment: Apart from the stated wide impacts on a range of issues, including personal privacy, national security and commerce, data localisation can also have a severe impact on economic freedoms accruing to parties. The World Economic Forum (WEF) for instance recommends countries to adopt open systems with

[3] UNCTAD, Data Protection Regulations and International Data Flows: Implications for Trade and Development, 2016, at <https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf>
[4] *Ibid*, p.104
[5] *Ibid* p.104-106
[6] Ikigai Law, The Data Localization Debate in International Trade Law, June 22, 2020, at <https://www.ikigailaw.com/the-data-localization-debate-in-international-trade-law/>
[7] *Ibid*

economic freedoms as the default.[8] Where this has not been done, countries have been encouraged to become signatories to international treaties like the Trans Pacific Partnership Agreement (TPPA) which expressly commit member countries to refrain from enacting data residency laws or local data centre requirements. International cooperation between intelligence and police forces, for example via Multilateral Assistance treaties, Executive Agreements under the U.S. Cloud Act, Interpol and regional cooperation arrangements also render data residency less relevant.[9] The report also recommends progressive solutions which empower governments to adopt policies that allow companies to participate in a globally-facing data economy whilst addressing governments' most pressing concerns of security, fairness and sovereign interest.[10] By implementing mechanisms to build trust the need to data residency laws is greatly reduced and the benefits of the data economy can be more fully realised.

Further, in a paper estimating losses that result from data localisation requirements estimated the GDP losses in India to be -0.8%, the impact on overall domestic investments to be -1.4%, and welfare losses (loss per worker) amounting to 11% of the average monthly salary, about 3.1-14.5 bn US$.[11]

Lastly, there is a requirement for an impact assessment of economic and other risks and benefits to be done before the implementation of a data centre policy. For instance, the Australian Government Data Centre Strategy 2010-2025 had outlined a savings target of $1 billion over a 15-year period. By 2017 the 2010-2025 strategy was on track to achieve its saving target.[12] Similarly, in Scotland, the Scottish Digital Futures Initiatives of 2012, 2015 and 2020, along with the Scottish Wide Area Network (SWAN) Programme have created a common approach to measurements and benefits.[13] The Measurement and Benefits Framework contains 16 measures, along with a 'benefits score card' which provides comprehensive coverage of the main benefits areas arising from the activity set out in the Scotland's 'Digital Future – Delivery of Public Services Strategy'.[14] This framework has been developed in partnership with Digital Public Service Strategy Assurance Board members and their sectoral boards and focusses on the key measurements and benefits to

[8] World Economic Forum, A Roadmap for Cross-Border Data Flows: Future Proofing Readiness and Cooperation in the New Data Economy, June 9, 2020,available at <https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy>
[9] *Ibid*
[10] *Ibid*
[11] Bauer, Lee-Makiyama, Marel and Verschelde, The Costs of Data Localisation: Friendly Fire on Economic Recovery, ECIPE Occassional Paper No 3/2014, available at <https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf>
[12] Australian Digital Transformation Strategy at <https://www.dta.gov.au/our-projects/hosting-strategy/overview>
[13] Information is available at <https://www.webarchive.org.uk/wayback/archive/20160104135654/http://www.gov.scot/Publications/2012/09/6272>
[14] Information on the 'Measurements and Benefits Framework' is available at <https://www.webarchive.org.uk/wayback/archive/20170104200054/http://www.gov.scot/Topics/Economy/digital/digitalservices/MandBframework>

deliver on the national priority action and strategic ambitions.[15] Therefore, there is a pressing need to conduct an impact assessment of costs and benefits of the extant Policy.

Therefore, it is proposed that instead of stringent data localisation mandates, the Ministry should introduce a strong data protection legislation to strengthen consumer protection and trust, and carry out a policy impact assessment of data localisation on small businesses, interoperability, and the data economy in India before implementing the Policy.

B. Digital Sovereignty

The emphasis on data localisation has also been linked to 'digital sovereignty' in clause 1.4 of the Policy. This is concurrent with the Government's larger "data sovereignty mission"[16], which can has severe impacts on the rights of people.

(i) Dissonance in judicial and policy perspectives on digital sovereignty: It is important to note that the assertion of digital sovereignty using data localisation mandates has been reiterated across sectoral policies including the RBI Notification on 'Storage of Payment System Data', the FDI Policy 2017, the Unified Access License, and the Companies Act, 2013 and its Rules, The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, the National M2M Roadmap, the draft PDP Bill, draft e-commerce policy, and the draft e-pharmacy regulations. This is largely incongruous with the judicial direction in *K S Puttaswamy and Anr* v *Union of India and Ors* [17](Puttaswamy), where there was a clear articulation of the right to privacy to be afforded to people in India as a matter of fundamental right. Therefore, in this regard, there is a lack of convergence that has been witnessed between the judicial position and legislative intent (through the PDP Bill) on the right to privacy and that of data as an economic asset to be exploited for national gains (as opposed to accruing to people as their individual right) and digital sovereignty under various extant Government policies mentioned above.[18]

Further, a study of most stakeholders in India has revealed that most civil society groups both in India and abroad, industry association bodies such as NASSCOM and Internet and Mobile Association of Indian, foreign stakeholders including technology companies and transnational

[15] *Ibid* 9
[16] Amber Sinha, Arindrajit Basu, The Politics of India's Data Protection Ecosystem, EPW Engage, Vol. 54, Issue No. 49, December 14, 2019,available at <https://www.epw.in/engage/article/politics-indias-data-protection-ecosystem>
[17] (2017) 10 SCC 1
[18] *Ibid*

advocacy groups have been ostensibly against blanket data localisation, in the form in which it is mandated by the PDP Bill.[19]

It has also been argued that to achieve the goal of digital sovereignty, fundamental pre-requisites need to established first, including a clear articulation of India's vision of the future of the Internet, incorporation of infrastructural and technical measures and standards, physical and logistical protection of data centers.[20] Further, it is recommended that since there are complex interlinkages of data availability, human capital and technological capability across multiple jurisdictions, policies mandating data localisation factor in this complexity by specifying clearly, the objectives to be achieved, and the alternatives for doing so.[21]

Therefore, it is recommended that a clear articulation of India's policy objectives on digital sovereignty is clearly articulated and harmonised with the legislative and judicial precedents and requirements.

(ii) Adequate protection of individual rights as a pre-requisite to digital sovereignty: The Puttaswamy judgement was fundamental in asserting that sovereignty of 'the State' arose from the sovereignty of people, through the mechanism of the Constitution of India.[22] In all the policies advancing digital sovereignty through data, including the present Policy, the arguments presented include advancing innovation or economic gains. While these claims have been contested above, it is unclear if the Policy considers user/citizen autonomy as a stated objective of digital sovereignty. An example to advance this argument is the lack of any mention of autonomy, privacy, cybersecurity, consumer and data protection in the present Policy. It is pertinent to note that it has been argued that without substantial protections and accountability measures, the present articulation of sovereignty in countries like India have echoes of colonial roots and cede excessive control of the people to the State and domestic private parties[23].

As such, it has also been urged that adequate protection for the rights of online users in India should be interpreted as a crucial aspect of data sovereignty.[24] The adequate protection of user's

[19] Basu et all, The Localisation Gambit, Unlocking Policy Measures for Sovereign Control of Data in India, Centre for Internet and Society, March 19, 2019, p. 48 available at <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>
[20] *Ibid* p. 62-63.
[21] Anirudh Barman, Lost in the Data Localisation Debate: Does India Have Full Power to Exploit its Own Data?, The Print, October 25, 2019,available at <https://theprint.in/opinion/lost-in-the-data-localisation-debate-does-india-have-full-power-to-exploit-its-own-data/310737/>
[22] *Justice K. S. Puttaswamy (Retd.)* and *Anr v. Union of India*, WP (Civil) No 494 of 2012.
[23] Anja Kovacs and Nayantara Ranganathan, Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India, Data Governance Network, Working Paper 03, November 2019,available at <https://datagovernance.org/files/research/IDP_-_Data_sovereignty_-_Paper_3.pdf>
[24] *Ibid* p. 63.

rights is especially relevant in the absence of a sector agnostic data protection law. In such a case, articulating a data centre policy, without a clear legal framework for the protection of user rights and strict data localisation mandates may also give rise to credible fears of surveillance by State authorities.[25]

It must also be noted that the operation of data centres necessitate the existence of strong cybersecurity laws in the country. In this regards, the General Data Protection Regulation in Europe, along with the EU Directive on Security of Network and Information Systems (NIS Directive)[26] create a strong ecosystem of trust, security and accountability. On the other hand, India has no single cybersecurity law or policy beyond a few scattered provisions in the Information Technology Act, 2000. The NIS Directive, amongst other things, establishes a reporting mechanism for cyber incidents. It impacts cloud providers in particular as there are provisions in the Directive for cloud platforms to be regulated, all of which are absent in India. Therefore, there is a requirement for such cybersecurity protocols and standards to be incorporated in India, to better service the needs of users and data centres.

Further, there should be an exploration of alternatives to better address the question of digital sovereignty, such as the adoption of the free software principles.[27]

As such, it is recommended that the extant Policy is framed within the context of a wider sector agnostic data protection law which details the various protections and safeguards available to users. This must be supplemented by strong cybersecurity standards and protocols. It is also recommended that the focus of digital sovereignty in the Policy through data localisation is realigned to focus on the autonomy of people, and alternatives to data localisation are explored.

[25] Bhandari, Vrinda, and Renuka Sane. "Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018." *Socio-Legal Rev.* 14 (2018): 143

[26] Directive on Security of Network and Information Systems (NIS Directive), Directive (EU) 2016/1148 of the European Parliament and of the Council, July 6, 2016, at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC>

[27] Sunil Abraham, The Fight for Digital Sovereignty, EPW, Vol-XLVIII No. 42, October 19, 2013

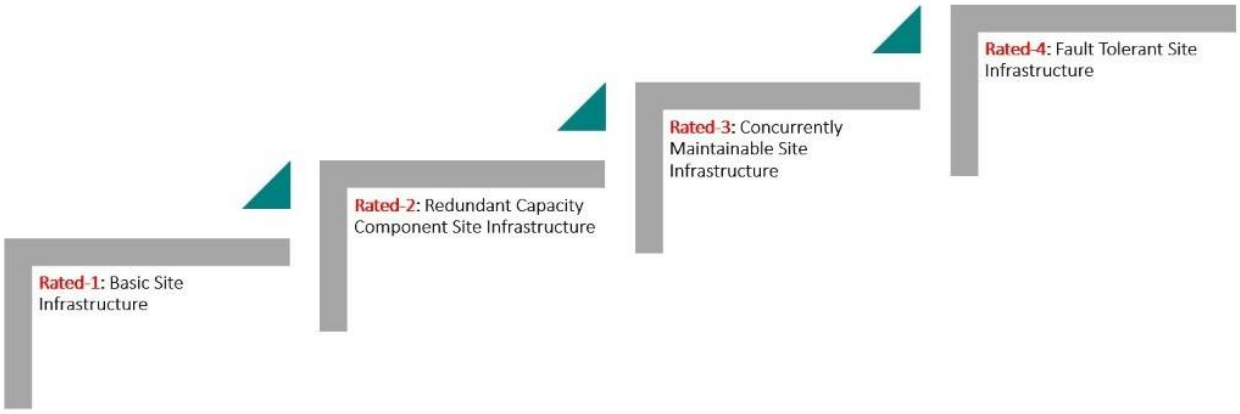
III. TECHNICAL STANDARDS

(i) Adopting Global Standards: At present there are three main sets of global standards that need to be followed for setting up data centres. These standards cover different aspects of a data centre (sometimes overlapping the areas covered) and enhance data centre reliability and overall performance. The standards were established by the Uptime Institute[28] (which uses a tier system), and include the ANSI/TIA 942-A 2014 standard, and the ANSI/BICSI 002-2014 standard.

The standards cover the infrastructure requirements for different types of data centre operations. The data centre classifications are divided into four tiers that "match a particular business function and define criteria for maintenance, power, cooling and fault capabilities. The Tiers are progressive, so each Tier incorporates the requirements of the lower Tiers". As explained by the Institute, the higher standards (Tier 4 as compared to Tier 3 for example) are not defined as an improvement over the lower standards but are defined with respect to different requirements. Companies/operators/regulators of the data centres have to choose the standards required for the infrastructure as per the specific use of the data centre. The facilities or components that are included in the different tiers deal with those related to power supply (provision of uninterrupted power supply, presence of generator sets in case of power disruption, fuel storage on location, etc.), cooling solutions for the equipment (cooling equipment which can run outside office hours, heat exchangers, heat rejection equipment, etc.), and redundancy solutions in case of outages.

Further, the ANSI/TIA 942-A 2014 standard "specifies requirements for data centers including single tenant enterprise data centers and multi-tenant Internet hosting data centers"[29] and encompasses "all physical infrastructure including, but not limited to, site location, architectural, electrical, mechanical, fire safety, telecommunication, security and other requirements"[30] The ANSI/TIA-942 standard serves as a baseline for anybody who wishes to design and build a reliable and efficient data center. ANSI/TIA-942 describes four Rating levels in which data centers can be classified. These are depicted in the diagram below[31]:

[28] Tier Classification System, Uptime Institute, Data Centre Classifications available at <https://uptimeinstitute.com/tiers >
[29] Telecommunications Industry Associations, Data Centre Classification available at <http://www.tia-942.org/ >
[30] ibid
[31] *Supra* 4



Finally, the ANSI/BICSI 002-2014 standard looks at specifications that data centres need to meet from the perspective of mechanical, electrical, and plumbing requirements of the physical infrastructure. It specifies the minimum requirements for each of these areas and covers the different aspects of planning, design, construction, and commissioning of the mechanical, electrical, and plumbing components along with the other aspects like fire protection, IT, and maintenance of the data centres.

In addition to these three main standards (which have been discussed briefly above), there are several other standards like the EN 50600 standards (a set of standards covering different aspects of data centres like building construction, power distribution, environmental control, telecommunications infrastructure, security systems, etc.), ISO 9000 standards (quality standards), ISO 14000 standards (environmental management system) and the ISO 27001 (information security) which are crucial for the functioning of data centres[32].

The present Policy does not detail which standards are going to be adopted for the efficacious management of data centres in India.

As such, it is recommended that MeitY considers adopting global standards to attract investment, while tailoring them both to suit the particular requirements of India, and for shaping future standards in the subcontinent. This also necessitates collaboration amongst various stakeholders, including the Government, companies, and academic institutions from various disciplines including engineering, law, policy and management.

(ii) **Requirement for legal and judicial reforms to support indigenisation:** Clause 5.1.5.2 of the Policy calls for incentives to be provided on usage of domestic IT hardware including servers, storage, network devices, etc. Further, clause 5.4.1.1 calls for promoting and encouraging the use of indigenous hardware. However, it is unclear if the definition of indigenous only covers

[32] Steven Shapiro, Data Center Design: Which Standards to Follow?, available at <https://www.datacenterknowledge.com/archives/2016/01/06/data-center-design-which-standards-to-follow>

what is manufactured in the country. If that understanding is correct, this might not lead to long-term sustainability since fabrication of high-end information technology (IT) and non-IT components is highly specialized, especially for IT components. Therefore, incentivizing large scale manufacturers of high-end computer hardware will need significant overhaul of several legal and judicial systems/processes.

Further, the cost of chip fabrication plants is often in the billions of dollars. For instance, China based SMIC announced in 2013 that it would be investing in a new semiconductor foundry (the largest in China at the time of announcement) that was estimated to cost USD 3.59 billion[33]. Toshiba Corporation had also announced that it would be investing JPY 195 billion (approximately USD 1.8 billion) in manufacturing equipment in the Phase – 1 clean room and construction of Phase – 2 of Fab 6 (suggesting that the cost of the entire Fab 6 unit would be higher)[34]. Similarly, Intel had projected that it would be investing USD 7 billion to complete a manufacturing facility that was originally announced in 2011 (which also implies that the cost of the facility is much higher)[35]. At present, Intel's plant manufactures 7 nanometre chips while the industry has started mass manufacturing 5 nanometre chips at present[36] and is exploring technology to start manufacturing 3 nanometre chips.

As such, it is evident that the up-front capital cost in setting up a chip fabrication unit are very high and the rate of obsolesence is similarly very high. Companies would be hesitant to invest such large sums unless there are strong IPR rights protections in the country.

Therefore, it is recommended that since setting up chip fabrication plants is a very investment heavy activity, laws protecting IPR and enabling efficient resolution of disputes be strengthened to increase market trust and attract investments. Thus, there is a requirement to improve IPR protection, speeding up dispute resolution including strengthening mechanisms of alternate dispute resolution.

(iii) **Requirement to institute environmental impact assessment system for data centres:** Several countries have instituted systems for enabling assessments on the impact of data centres on the environment. Data centres and cloud computing have a heavy footprint featuring high

[33] Shih, T. H. (2013, June 4). *Chinese semiconductor maker SMIC plans US$3.59 billion Beijing plant*. Retrieved November 19, 2020, from South China Morning Post: available at < https://www.scmp.com/business/china-business/article/1252888/chinese-semiconductor-maker-smic-plans-us359-billion-beijing>

[34] Toshiba Corporation. (2017, August 3). *Update on Toshiba Memory Corporation's Investment in Production Equipment for Fab 6 at Yokkaichi Operations.* Retrieved November 19, 2020, from Toshiba: available at <http://www.toshiba.co.jp/about/ir/en/news/20170803_1.pdf>

[35]Intel Corporation. (2017, February 8). Investing in the future of Moore's Law. Retrieved November 19, 2020, from Intel | Data Center Solutions, IoT, and PC Innovation: available at < https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/02/investing-in-the-future-of-moores-law.pdf >

[36] TSMC. (n.d.). 5nm Technology. Retrieved November 19, 2020, from Taiwan Semiconductor Manufacturing Company Limited: available at < https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_5nm >

consumption of non-renewable energy, waste production and CO_2 emissions[37]. It is recommended that there be a system for India as well to assess the impact data centres will have on the country's resources. There are several examples of such impact assessments including the 'Building Research Establishment Environmental Assessment Method' (BREEAM) in the UK[38], and 'Green Globes'[39] in Canada and the US, 'Hong Kong Building Environmental Assessment Method' (HK-BEAM)[40] in Hong Kong,'Ecology, Energy Saving, Waste Reduction, and Health' (EEWH)[41]in Taiwan, 'Green Mark'[42] in Singapore, and 'National Australian Built Environment Rating System' (NABERS)[43] in Australia and 'Comprehensive Assessment System for Building Environmental Efficiency' (CASBEE)[44] in Japan.

It is thus recommended that environmental impact assessment is made a regulatory requirement for data centres to measure the impact on carbon footprint and the environment.

[37] Lucivero, F. Big Data, Big Waste? A Reflection on the Environmental Sustainability of Big Data Initiatives. Sci Eng Ethics 26, 1009–1030 (2020)

[38]Building Research Establishment Environmental Assessment Method, available at < https://www.breeam.com/>

[39] Green Globes Assessment Method, available at <http://www.greenglobes.com/home.asp>

[40]Hong Kong Building Environmental Assessment Method, available at <https://www.beamsociety.org.hk/en_about_us_0.php>

[41] Measuring Green Data Centres, Chapter 2, Pg 45 available at <https://cdn.ttgtmedia.com/searchSystemsChannel/downloads/Growing_a_Green_Data_Center_9781587058134_CH02.pdf>

[42] Building and Construction Authority, Green Mark Scheme, available at <https://www.bca.gov.sg/greenmark/green_mark_buildings.html>

[43] National Australian Built Environment Rating System available at, < https://www.nabers.gov.au/>

[44]Comprehensive Assessment System for Building Environmental Efficiency, available at , <http://www.ibec.or.jp/CASBEE/english/>

(iv) **Requirement for upscaling infrastructure provisions and conducting ecological and environmental impact assessments**: The estimated electricity usage by the entire global data centre industry in the year 2018 was 205 TWh (or 1% of global electricity consumption)[45]. The total energy consumption in India in 2018 was 1308.146 TWh and in 2019 was 1376.095 TWh[46]. According to a report by the Lawrence Berkeley National Laboratory, the electricity requirement for the data centres in the United States was estimated to be approximately 70 TWh in 2018[47].

The report also estimated that data centres in the US would consume approximately 660 billion litres of water in 2020[48]. The United States consumes this amount of water while housing 47% of the world's hyperscale cloud data centres (as of Q2, 2016)[49]. India with a market share of just 3% would have needed access to 42.13 billion litres of water in 2020 (assuming that the market share remained the same from 2016 to 2020)[50]. This is a very large amount of water that is needed for the existing data centre operations in the country. If we are to successfully attract more data centres, this will require us to provide access to good quality water for the data centres to use for cooling purposes. At the same time, the global data centre industry is expected to be contributing around 0.3% to overall carbon emissions[51]. Hence, the ecological impact of the large quantities of water consumed as well as the emissions needs to be further studied.

As such, this data shows that there is a requirement for large quantities of uninterrupted power and water for data centres to function optimally. Given the Government's push towards making India a destination for data centres across the world, adequate availability of electricity and water will have to be ensured to data centres. Unfortunately, states which have access to perennial river systems do not always have the most reliable electricity grids and vice-versa. India ranked 96 out of 141 countries on the reliability of its water supply in 2019[52]. India also ranked 105 out of 141 countries in access to electricity and 108 out of 141 in quality of electricity supply according to 'The Global Competitiveness Report, 2019'[53]. This factor was also taken into consideration by NASSCOM when they recommended establishing "dual power grid networks to ensure uninterrupted supply of electricity"[54].

> *Therefore, it is recommended that improving the status and quality of the power infrastructure in the country should be made a pre-requisite for the implementation of the Policy. Further, there is also a requirement to improve the supply of water resources and streamline the mechanisms for resolving water disputes between states. Also, since high volume water sources are needed and the land parcels need to be ideally close to river systems or large bodies of water, there is an unqualified requirement to study the ecological and environmental impact of data centres in India.*

IV. INSTITUTIONAL MECHANISM FOR POLICY GOVERNANCE

The Policy in clause 5.5 details the creation of an inter-ministerial empowered committee (IMEC) under the aegis of MeitY, to be the key decision-making body to facilitate the implementation of various measures detailed in the said Policy. The details of members of the IMEC, tenure and terms of reference are to be notified by MeitY.

(i) Requirement for a Data Protection Authority to be Nodal Agency: It is appreciated that there has been a concerted effort to streamline the institutional mechanism for policy governance in the Policy. However, it must be noted that the white paper issued by the 'Committee of Experts' under the Chairmanship of Justice B.N. Srikrishna suggested the creation of an independent regulatory body for enforcement of a data protection legal framework. Further, it was suggested that this regulatory body should have the powers of (a) monitoring, enforcement and investigation; (b) awareness generation; and (c) standard setting. The report also detailed a number of regulatory tools and mechanisms such as codes of practice and categorisation of data fiduciaries could be deployed to achieve enforcement objectives.[55] Therefore, in light of the proposed 'Data Protection Authority' (DPA), which is to function as a sector-agnostic, "high-powered, independent national body in view of the significance of creating an ecosystem of responsible data handling", creation of the IMEC may not serve as an appropriate mechanism under the extant Policy.[56] It can also be argued that because of the absence of a legal framework to govern the constitution and functioning of the IMEC, stakeholders may be unable to participate and advance the objectives of the policy. It must be noted that in several countries including the UK, USA, Singapore and Australia, data centres are separately regulated, but come under the aegis of the privacy and data protection legislation in the respective countries. This is further supported additionally through specific policy initiatives.[57]

Further, for inter-sectoral coordination, the white paper envisaged a consultative framework of policy making, wherein the DPA would consult relevant regulators and authorities including state

[55] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians, Data Protection Committee Report, 2018, p. 158.
[56] *Ibid*

[57] Examples of such additional policy initiatives include the 'Federal Data Center Consolidation Initiative' in the US (see FITARA section 834), the 'Japan Data Centre Council' in Japan, and the Digital Public Services Programme Board for National Level Actions and the Digital Public Services Strategy Assurance Board in Scotland.

governments, before taking any action under the proposed data protection legal framework and also enter into a memorandum of understanding with such regulators and authorities.[58]

As such, it is recommended that instead of the IMEC and the proposed 'Data Centre Facilitation Unit' (DCFU), the Ministry consider making the proposed DPA the nodal agency to regulate and co-ordinate all data centric policy implementation. The IMEC and DCFU can also seek to assist the DPA in carrying out its functions.

(ii) Requirement for Due Consultation with Stakeholders: It must also be noted that the Handbook by the Cabinet Secretariat[59] also details the structures of inter-ministerial consultation for proposals that are placed before the Cabinet and Committees of the Cabinet. These consultations are to be held with the stakeholders within the Central Government and outside, consultations with the state governments, inter-ministerial consultations and in many cases, appraisal by designated bodies or financial institutions. In this regard, given the environmental impact of data centres (outlined in issue II of this submission under the heading of 'standards'), it is essential that the DPA along with the IMEC should mandate consultation and representation in the IMEC from the Ministry of Environment, Forest and Climate Change. Further, it is also recommended that the Ministry of Power, Ministry of Labour and Employment, Ministry of Waterways and the Department of Telecommunication are also consulted on any policy pertaining to data centres.

Further, given that data centres will be located in multiple states across the country, utilising land, electricity, water and other resources of states, it is pertinent that adequate consultation is carried out with state governments. In this regard, the Japan Data Centre Council which is an independent council consisting of both governmental bodies and leading companies[60] is a good example for setting up an independent organization solely for the purpose of data.

Therefore, it is proposed that the IMEC envisaged under the Policy, along with the DCFU and the Data Centre Industry Council mentioned in clause 5.5.2 of the Policy should act as a supplemental forum of policy governance, to support the primary regulatory functions undertaken by the DPA, with due consultation from other relevant Government bodies and ministries, and relevant state governments.

[58] *Ibid*, p. 158
[59] Government of India, Cabinet Secretariat, Handbook on Writing Cabinet Notes, Section 4, p 39.
[60] Information at <https://www.jdcc.or.jp/english/index.html>