GNLU CENTRE FOR LAW & ECONOMICS

Policy Recommendations

GNLU/CLE/PR-03
27 February 2022

Recommendations to the Ministry of Electronics and Information Technology on Indian Digital Ecosystem Architecture 2.0

Comments on behalf of the Centre for Law & Economics

Centre Faculty

Prof. (Dr.) Ranita Nagar
Professor of Economics
Head of Centre for Law & Economics

Dr. Hiteshkumar Thakkar
Assistant Professor of Economics,
Co-Convenor, Centre for Law & Economics

Student Members

Debargha Roy
Niharika Agarwal
Adya Desai
Aishita Yadav
Shivanshi Tyagi
Bhawini Jha
Anmol Singh Gaur

© GNLU Centre for Law & Economics, Gandhinagar, February 2022.

Index

I. Introduction

The Ministry of Electronics and Information Technology (MeitY) released the India Enterprise Architecture (IndEA) 2.0 Framework with an aim to "establish best-in-class architectural governance, processes and practices with optimal utilization of ICT infrastructure and applications to offer ONE Government experience to the citizens and businesses" in January 2022, soliciting comments from stakeholders and members of the public. Keeping in mind the mandate of the Centre for Law and Economics at the Gujarat National Law University, Gandhinagar, an endeavor was made to study and analyze the Framework in order to provide comments for regulating the crucial space of information technology, data protection and privacy governance. There is a clear focus in the framework to enhance the digital governance vision with a view to ensure that every step of governance can be integrated with technology.

Therefore, the Centre for Law and Economics constituted a Research Group on the IndEA Framework and research on the recommendations to suggest comments. This document is a collection of the comments of the Research Group, where the focus of the group was to strike a balance between enabling effective digital governance on one hand and protecting the data of users in line with the privacy and data protection developments in India and around the world. This was done through highlighting efforts were made to collate and scrutinize the working of data protection and privacy developments in international jurisdictions, which are also incorporated in the Specific Comments advanced below. We sincerely hope that our comments are valuable to the concerned stakeholders.

II. General Comments

The present section provides certain general comments advanced by the Centre on the InDEA Framework. The draft, although comprehensive in laying down a framework for digital governance in India, has certain areas that it could further throw light upon. With release of the recommendations on data protection by the Joint Parliamentary Committee in December, 2021,[1] there is scope for aligning the Framework further

[1] Lok Sabha Secretariat, *Report of the Joint Committee on the Personal Data Protection Bill, 2019,* Lok Sabha, Government of India (Sept. 16, 2021), http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf [hereinafter "*Report*"].

towards the recommendations and upcoming developments in the Data Protection Bill, 2019[2]. At an ecosystem level, there must be scope for users to grant clear permission before the data by the user is exchanged between various levels. The user must be informed about what specific objectives the data seeks to serve in the ecosystem. There is also a need for the user to see all data collected under the Digital ID in a readable format and have the right to retract data on demand in accordance with the Supreme Court precedents in data protection. Certain specific suggestions have been highlighted in the specific comments following this section.

While the framework integrates the technology related developments with governance towards delivery of services to citizens and businesses, there is more scope in building a stronger obligation for the Government towards the protection against misuse of the data of users. As per the recent IRDAI regulations pertaining to cyber insurance, cover has also been provided for data and privacy breaches as well as for Malware and data restoration costs. Indemnity has been provided for defense costs and damages in respect of claims lodged by a third party against the Insured for Data Breach and or Privacy Breach.[3] In light of the increase in the number of cyberattacks on personal computer networks and routers during the COVID-19 pandemic period as per IRDAI circular issued 8th September 2021[4], it is important for clear legal provisions pertaining to the specific liability for data breaches within this linked ecosystem especially taking into account the participation of multiple stakeholders of public, private and foreign entities within the ecosystem. It is necessary also to explicitly lay down for the private companies participating within the ecosystem the guidelines for insurance, indemnity and liability as the multi-layered system so as to continue incentivization of their participation in data exchanges, and data sharing frameworks, while simultaneously restricting the extent of the same to uphold the data security of consumers.

There is further scope for integration of public-private participation in data sharing procedures which are clear and adherent to the data protection jurisprudence. For instance, the 'sandbox' as found in the Data Protection Bill, 2019 could be further elaborated in this Framework to foster private players in developing robust innovations for communities and society. Similarly, there is also scope for encouraging private and public counterparts in the insurance industry to enable data insurance policies. Bigger business establishments could further have financial incentives when they adhere to additional data protection compliances towards a model data management policy.

---

[2] The Personal Data Protection Bill, 2019, § 33, § 34, No. 373, Acts of Parliament, 2019 (India), [hereinafter "Bill"].

[3] Yegnapriya Bharath, Chief General Manager (Non-Life), IRDAI, Chief General Manager (Non-Life), Product *Structure for Cyber Insurance Circular,* INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA (Sept. 8, 2021),https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo4560&flag=1.

[4] IRDAI, *Guidance Document On Product Structure for Cyber Insurance,* INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA (Sept. 8, 2021), https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo4560&flag=1

Keeping in mind the broad vision set by the Framework, the aforementioned comments have been made, keeping in mind the active participation of the Government in robust data governance.

III. Comments on Section 2 InDEA Principles

Sec No. (Of draft)	Proposal by MeitY	CLE Research on Comments	Final Comment
2.4.3.	Data is an asset: Design data systems in a manner that creates, supports, maintains, and enhances value to the enterprise specifically, and to the ecosystem in general. · Promote establishment of Data Exchange(s) that enable regulated exchange of data for public purposes, innovation, and research, and for permitted commercial purposes. · Establish / promote robust data governance	a. As per the personal data protection bill, the processing of personal data does not explicitly allow for Data Exchanges as proposed in section 2.4.3.[5] b. Section 12 of the Personal Data Protection bill requires the valid consent of the data principal for the purpose of processing also, the data to be processed can be sensitive personal data which requires an explicit consent from the principal.[6] c. Section 5 of the PDP bill sets clear limitations on the purposes for which	a. The term data exchanges needs to be unambiguously defined so as to prevent data laundering. b. An active and robust system of consent collection is necessary, so as to make the process legally accurate. The term "permitted commercial purposes" needs to be unequivocally defined and information for the same must be freely available to all

[5] Bill, *Supra* note 2.
[6] *Id.*

	systems in conformity with the best practices	data may be processed. Section 7 lists out the requirements for lawful processing as further elaborated in chapter 3&4. None of the sections under the chapters allow for "processing for commercial purposes". [7] d. In the case of Justice K.S Puttaswamy v. Union of India, AIR 2017 SC 4161, the honorable Supreme Court observed that the individual alone has the right to control and commercially exploit the information present about them online and therefore if the data of an individual is shared with private entities and they use it for data monetization then it would be better if the individuals are paid for using their data so as to move towards the phase where data is treated same as the property and individuals can derive economic benefits from them.	citizens and such purposes also need to be regulated. c. The stand on use for commercial purposes needs to be altered to be compatible with the PDP bill. d. Recognize the principle of monetization of data by users as recognized by the Supreme Court.

[7] *Id.*

2.4.4	Data Sharing Lay down clear data sharing policies specific to the relevant domain(s), that enable and regulate the sharing of data, in conformance with the applicable data protection regulations. Data sharing policies apply to public sector data Private sector may adopt the data sharing policies on a voluntary basis.	The Draft Personal Data Protection Bill states that its laws are only applicable to body corporates located within India. The policy of data exchange among private entities which may be participating in a given sector and having consumers located in India, as well as collecting data from said consumers, but not having a physical presence may not be subject to these laws.[8] The access to various forms of data through this data exchange policy by such foreign companies could therefore pose a threat to user privacy and security aimed in sections 2.4.6 and 2.4.7 respectively. As per The Joint Parliamentary Committee Report, India's information technology sector is highly integrated with global data flows with 8 of the 10 most accessed websites in India belonging to US based entities. Most of the data in such interactions can currently be stored, processed and transferred around the world. Moreover, the access, storage and transfer of this data by companies abroad would contradict the aim of data localization put forward by both the RBI in its 2018 mandate as well as the government in the draft	The principle of data localization should be kept in mind so as to limit data exchanges to foreign entities. Mechanisms should be established to ensure localization of data adhering to the proper categorization to restrict its access to foreign entities.

		Personal Data Protection Bill, 2019 under section 33. The Joint Parliamentary Committee Report recommends localization of data through categorization as sensitive and critical personal data and hence restrict access to it by foreign entities under section 11. It stressed on the need to do so for the purpose of national security, employment generation, as well as upholding the privacy of citizens which it has placed as a priority above promotion of business. Article 33 and 34 of the PDP Bill lays down the relevant conditions for the transfer of data abroad, based on its categorization as critical or sensitive data, which must be addressed.	

2.4.6.	Privacy-by-Design: *Design and publish a privacy policy that conforms to the principles of Privacy-by-Design.* o Privacy-by-design implies adopting the nine principles listed below o Notice o Choice and consent o Purpose limitation o Collection limitation o Access and correction o Security o Openness, transparency and o Accountability	The given proposal does not consider the principle of the "Right to be forgotten" within the "Right to privacy". Internationally this right was established by the landmark case "Google Inc v Agencia Española de Protección de Datos, Mario Costeja González (2014)". Thereafter it has also been codified by the GDPR (General Data Protection Regulation) along with the right to erasure.[9] - The law calls for erasure of data as soon as it is no longer needed for its original processing purpose if there are no legal grounds for its processing or the data subject has objected. *Therefore, if the data has been linked with any secondary processing purpose, then this may create obstacles to the same when the data would have to be erased following the completion of the original processing purpose. This must be considered in the context of centralized*	The right to be forgotten should be recognized.

[9] Intersoft Consulting, *GDPR Right to be Forgotten,* INTERSOFT CONSULTING, (Accessed: Feb. 25, 2022, 9:12 PM) https://gdpr-info.eu/issues/consent/.

		and shared data systems. - Article 17 (2) of the GDPR also mandates that if the controller has made the personal data public, and if one of the above reasons for erasure exists, the controller must take reasonable measures, considering the circumstances, to inform all other controllers in data processing that all links to this personal data, as well as copies or replicates of the personal data, must be erased. *This, when applied to the data network and ecosystem envisioned by the proposal, necessitates mechanisms to ensure that shared or duplicated data is also adequately erased.* - Furthermore, it also enables the data subject to withdraw their consent at any point following which any collected data may be erased at the choice of the data subject. *There must therefore be mechanisms recognizing this right,*	

		at any stage of data processing, sharing or storing. - The Joint Parliamentary Committee Bill also establishes the need for technological systems that may be able to efficiently implement such laws and ensure the Right to be forgotten by citizens. [10] Therefore, the proposal must account for the same and include mechanisms for implementing them.	
2.4.6	Consent	The GDPR within Article 7 and recital 32 lays down the various elements of consent that must be present during personal data processing. While the proposal mentions the importance of consent itself, it does not explicitly provide mechanisms for the implementation of each of these aspects of consent. [11] 1. The consent must be free. By this, it is meant that the consumer must have a real choice without coercion or influence that would affect the	Keeping in mind the guidelines laid out in the GDPR which have also been referred to in the PDP Bill and the Joint Parliamentary Committee Report, it is suggested that the framework for consent be more specifically and elaborately addressed within the framework specified in the report so as to ensure the Right to privacy of individuals

[10] *Report, Supra* note 1.
[11] Intersoft Consulting, *GDPR Consent,* INTERSOFT CONSULTING, (Accessed: Feb. 25, 2022, 8:20 PM) https://gdpr-info.eu/issues/consent/.

		outcome of the choice made. In this context there is a “coupling prohibition”. As per recital 43 clause 2, consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance. 2. Consent must be informed and specific. Therefore, along with purpose and collection limitations, it is important for the controller’s identity, as well as information about how the data will be used to be notified. Under the GDPR, where relevant, the controller also has to inform about the use of the data for automated decision-making, to avoid the possible risks of data transfers due to absence of an	is upheld to the highest degree.

		adequate decision or other appropriate safeguards. 3. Consent must be explicit, in clear terms and not implied or ambiguous. It is also important for the process to be “opt-in” rather than “opt-out” such that there is an active declaration that is agreed upon. 4. For minors and individuals of unsound mind who are not capable of legally providing consent, there must be provisions for additional authorization from a guardian.	

IV. Comments on Section 4 Federated Digital Identities

Sec No. (Of draft)	**Proposal by MeitY**	**CLE Research on Comments**	**Final Comment**
4.2.3	All digital platforms require master data and actor (person/entity/thing) data related to that system to be maintained for identification, validation, etc. For example, a	The benefits of a registry are clear. However, there are certain security precautions that must be taken when handling large amounts of sensitive data. The report advocates for privacy-by-design and security-by-design principles but does not clarify how and where the	

	property tax system needs to maintain master data about properties, the PDS system needs to maintain master data about the beneficiaries and so on. As the world becomes data rich, it is essential that various data about people, entities, geographies, resources, assets, etc. are made available in electronic registries with Open APIs for other applications to seamlessly validate and use attested and authenticated data. This is even more critical when it comes to people and entities where various claims can be electronically validated against such registries via open APIs avoiding paper-based validations, thus increasing trust while decreasing cost of validation. In this document, the word “Electronic Registry” is used to depict a trusted system that enables consented subjects (people,	data will be stored and whether or not it will be encrypted. Further, it should be clarified how the data will be validated through the Open APIs. If it gives access to the data, then consent is necessary. However, the ZK proofs can be potentially used to validate documents without sharing sensitive information.	

	entities, things) to enrol, manage their record with necessary levels of verification, and avail 3rd party services built on it using its authentication and KYC services. Aadhaar is a registry of “usual residents of India”, PAN system is a registry of “persons (people/entity) who are direct taxpayers”, PDS database is a registry of “people (and families) who receive food subsidy”, and so on.		
4.3	Recommendations on Federated Digital Identity Ecosystem 3. Handling uniqueness: a. When global state-controlled uniqueness is necessary, allow users to link their Aadhaar or other Aadhaar linked or Aadhaar derived or Aadhaar based digital IDs to achieve it. b. If not (if it is user-controlled uniqueness), then	Section 4.2.2 describes what is to be understood as State controlled uniqueness which indirectly refers to the AADHAR. Since the Personal Data Protection bill is not applicable to the Aadhaar Act as the draft report by the B.N.Srikrishna Committee which was constituted in the wake of the landmark “Right to privacy” judgement by the Supreme Court to come up with a data protection framework states that the legislation would not apply to any processing activity that had been completed prior to this law coming into effect**.** Thus the	

	allow common identifiers such as mobile numbers or other acceptable Digital IDs to be used and still allow users to voluntarily use their Aadhaar. c. This allows minimizing the need to remember and use many IDs by the citizens and provides the convenience of managing their account using either Aadhaar or mobile or other acceptable digital IDs.	proposed Personal Data Protection bill shall not be enforced retrospectively, therefore there is a considerable loophole in the privacy of an individual if state controlled uniqueness is made necessary as a registry in any digital ecosystem. This leaves the person with no control over their privacy.[12] Thus a user controlled uniqueness must be used to the greatest extent possible and even in cases where there is a need to rope in state controlled uniqueness it must be used in combination with user controlled uniqueness.	

[12] Bill, *Supra* note 3.

GNLU CENTRE FOR LAW & ECONOMICS

Gujarat National Law University, Attalika Avenue, Knowledge Corridor, Koba, Gandhinagar – 382007, Gujarat, India

Ph: +91-79-23276611/12, Fax: +91-79-23276613, Email: cle@gnlu.ac.in
Website: https://gnlu.ac.in/Law-And-Economics/Home