The Centre for Internet and Society's comments and recommendations to the:

Data Empowerment and Protection Architecture

30th November 2020

By: Shweta Reddy, Pallavi Bedi, Anubha Sinha, Shweta Mohandas

The Centre for Internet and Society, India

Introduction

The Centre for Internet and Society (CIS) is a non-profit research organisation that works on policy issues relating to privacy, freedom of expression, accessibility for persons with diverse abilities, access to knowledge, intellectual property rights and openness. It engages in academic research to explore and affect the shape and form of the Internet, along with its relationship with the Society, with particular emphasis on South-South dialogues and exchange. CIS has conducted extensive research into areas such as privacy, data protection and data security.

CIS is grateful for the opportunity to submit its inputs on the draft Data Empowerment and Protection Architecture (DEPA report).

Proposed data protection framework and DEPA

1. **Absence of a comprehensive policy framework:** The DEPA report like the report on the National Digital Health Mission is another policy report concerning the use of personal data that has come in the absence of a data protection law. The report states that informed consent, data minimisation, data portability and accountability of the data fiduciary are a part of the guiding principles of the DEPA framework. These terms have not been defined in the DEPA report, however, they have been defined under the PDP Bill. The PDP Bill also stipulates the accountability and transparency measures that data fiduciaries are required to adopt. Since the proposed PDP Bill has defined these terms and has also stipulated measures to be adopted by the data fiduciaries to ensure compliance with such provisions, the need for a separate DEPA framework (especially in the absence of the proposed PDP Bill) is unclear.

   There is also lack of clarity in the relationship between the PDP Bill and the DEPA framework- significantly, the role of the proposed Data Protection Authority and whether the Data Protection Authority will have the supervisory/regulatory power over the different sectoral DEPA frameworks.

2. **Lack of clarity on the range of functions of consent manager:** The concept of consent managers has been introduced in the proposed data protection framework and has been defined as "a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform."[1] Based on a plain reading of the definition, it appears that the nature of functions of the consent manager shall be very narrow. The power to issue further regulations on the technical, operational, financial and other conditions for registration of the consent manager is with the (yet to be established) Data Protection Authority[2]. Currently, the functions of the

[1] Section 23, Personal Data Protection Bill, 2019
[2] Section 94(h), Personal Data Protection Bill, 2019

consent manager, as mentioned, in the definition do not dilute the obligations of the data fiduciary and data processor.

In the proposed DEPA framework, in addition to performing the role of managing and recording consent, the architecture of the consent manager is said to replace cumbersome data sharing practices such as the terms and conditions forms providing blanket consent[3]. It is currently unclear if the consent manager is expected to summarize the terms and conditions for the benefit of the data principal and the negotiating power that the consent manager is expected to possess to ensure blanket consent is not asked for by the information users. If the consent manager is summarizing the terms and conditions and by extension the privacy policies of the information user, the impact of such a function on the notice obligations of the information user will have to be examined. It is essential that the broader data protection obligations on the information users and providers is not diluted due to the functions of the consent managers.

The consent managers have been given the power to build multidimensional trust rating scores for information providers and users[4]. These trust scores seem to be similar to the data trust scores under the proposed data protection framework. Under the said framework, a data auditor registered with the data protection authority is expected to provide the data trust score based on the criteria determined by the DPA[5]. It is unclear if the trust rating scores under the DEPA framework are different to the data trust scores under the proposed data protection framework. If they are different, the credibility of a consent manager and their subject matter expertise and accompanying procedure to award such scores should be clearly laid out. Questions around how such trust scores are expected to work in case of multiple consent managers for every information provider and user should be addressed. If the trust rating scores under the DEPA framework are similar to the data trust score of the proposed data protection framework, the overlap between the obligation of the data protection authority and the function of the consent manager and a strong case for the latter's credibility over a registered data auditor in providing such scores should be made.

3. **Lack of clarity on the role of consent managers if the legal ground for data processing is not consent:** The primary objective of the DEPA framework is to "grant users control over data through a safe and seamless protocol to share data across institutions, leading to individual empowerment and well being."[6] The consent managers can manage and record consent in cases where the information users are relying on consent as the legal basis for processing personal data. The proposed data protection framework, in addition to consent, allows for various other lawful grounds of processing. Additional research on the potential loss of control in event of relying on the other lawful grounds should be conducted to

[3] Data Empowerment and Protection Architecture, Page 3
[4] Data Empowerment and Protection Architecture, Page 49
[5] Section 29(5),Personal Data Protection Bill, 2019
[6] Data Empowerment and Protection Architecture, Page 25

determine if the consent manager, in an effort to look out for individual data interests, can aid in enabling control in such a situation as well.

4. **A self-regulatory organization consisting of consent managers, data providers and consumers may not be feasible:** The framework suggests creating a self-regulatory organization consisting of consent managers, data providers and consumers which shall be tasked with the responsibility of addressing user interests, designing sector specific data sharing guidelines and monitoring compliance by all players[7]. The framework omits a vital detail by not addressing the interaction between the self- regulatory organization and the (to be established) data protection authority(DPA) since the players operationalizing the framework fall under the jurisdiction of the DPA. The provision for developing codes of practice[8] under the proposed data protection framework can ensure that any sector specific guidelines in relation to the consent manager can be approved by the Data Protection Authority and the Authority can ensure compliance. It is also unclear why the functions that are to be performed by the self-regulatory organization cannot be performed by the DPA since this very clearly falls within their mandate according to the proposed data protection framework.

5. **Clarity on why data portability sections of the proposed data protection framework cannot disable data silos:** It has been contended that individuals have to rely on a patchwork of work around solutions to access data that is stored in different formats[9] and lack of clear guidelines on porting data accentuated the process. The proposed data protection framework requires data fiduciaries to provide data principals with their personal data in a structured, commonly used and machine-readable format and also have such data transferred to any other data fiduciary based on the request of the data principal. The section on codes of practices of the proposed framework permits such codes to determine the standards and means of exercising their right to data portability[10] which should allow for sector specific portability standards, if required.

   Since the proposed data protection framework has provisions aimed at breaking data silos at the request of the data principal, it is unclear if the proposed DEPA framework is recommending any additional steps in aiding the existing proposals.

[7] Data Empowerment and Protection Architecture, Page 35
[8] Section 50 Personal Data Protection Bill, 2019
[9] Data Empowerment and Protection Architecture, Page 26
[10] Section 50(6)(j) Personal Data Protection Bill, 2019

Other comments

1. **Sector specific adoption of the DEPA framework:** The DEPA report states that it is ' a secure consent based data sharing framework to accelerate financial inclusion'. DEPA is seen as the final layer in India Stack- the other two being (i) identity proof through Aadhaar and (ii) mobile digital payment through the Unified Payments Interface in 2016. The report in the section titled 'roadmap' states that DEPA will also be adopted by other sectors- namely health, telecom and skills data. The legal and regulatory section of the report is silent about the legal and regulatory framework for deploying the DEPA framework in different sectors other than the financial sector.

   The architecture envisaged by the framework appears to be concentrating on financial inclusion, there is no clarity on whether this architecture/framework will be applicable across other different sectors. As per the report, the National Health Authority (NHA) has been tasked with implementing the National Digital Health Mission, and is piloting the DEPA architecture for healthcare data. However, no information has been provided as to the mechanism/architecture to be followed by the NHA for adopting a DEPA model based on the financial sector to the health sector. It is also important to note that the DEPA model and report identifying the NHA as the authority responsible for piloting the DEPA model in the health sector has been published at a time when public comments were invited on the Health Data Management Policy which seeks to give a health id to the data principle.

   As per the DEPA report, in case of unregulated sectors (such as e-commerce, education), consent managers will be created by the Data Protection Authority, however, in case of regulated sectors, consent managers will be created by sectoral regulators. Under the proposed Personal Data Protection Bill, 2019, consent managers have to be registered with the Data Protection Authority[11]. The DEPA report is silent on whether the consent manager created by the sectoral regulators will need to register with the Data Protection Authority.

2. **Role of civil society:** Civil society has been asked to serve as an "alert watchdog" for data sharing practices. However, the exact nature of potential collaborative efforts have not been outlined. The efficiency of civil society as an external "watchdog" is severely limited when they haven't been involved extensively in the design and development stage of the framework. The involvement of civil society in the drafting and creation of the framework is essential to allow civil society to define and understand their place in the framework and the ecosystem of stakeholders, and enable any sort of external scrutiny.

[11] Section 23(5), Personal Data Protection Bill, 2019

3. **Advisable to rely on a business model that doesn't rely on charging individuals for services:** Charging individuals for services is one guaranteed method to ensure competition in the market which will further ensure that there isn't a service provider lock in. However, since the primary objective of the DEPA framework is to aid in giving back the individual control over their personal data, (which is an essential tenet of the right to informational privacy) charging individuals for such a service can make privacy accessible only to those who can afford it. Even though the existing Account Aggregators do not charge for their services, an indication that the business model could rely on fees in the overarching framework can result in deepening the digital divide by eliminating service to certain poorer sections of the demographic. The other option of charging Information Users for their services can be considered as a more feasible option.

4. **Heavy reliance on the traditional notice and consent model:** The proposed DEPA framework relies heavily on the notice and consent model. It doesn't take into consideration the current conversations around revisiting the idea of consent[12] to incorporate variable characteristics such as the social context of the individual, the cognitive limitations in an individual's ability to make informed choices, consent fatigue and lack of bargaining power in a transaction[13] resulting in a mere illusory control over disclosure of personal data. The proposed framework is expected to cater to a wide demographic but doesn't take into consideration the digital and linguistic divide in the country which can make individuals using online services for the first time extremely vulnerable as the framework assumes that all individuals are in a position to understand the consequences of the consent they are providing. Such persistent challenges, including the one of long and complex privacy policies (most of them in English), are not addressed by the consent manager model. Hence relying on only consent to ensure data empowerment might not be advisable.

5. **Compatibility with feature phone usage:** One of the most consistent feedback for the DEPA framework and the Account Aggregator model has been the importance of ensuring the architecture takes into consideration the different patterns of phone usage across the country and that the consent interface is compatible with feature phone usage[14].

6. **Lack of clarity on the regulatory architecture of the DEPA framework:** The report is silent about the regulatory framework of DEPA across the different sectors. It relies

---

[12] Anja Kovacs and Tripti Jain, "Informed consent - said who? A feminist perspective on principles of consent in the age of embodied data" *Internet Democracy project,* November, 2020, https://datagovernance.org/files/research/1606218143.pdf

[13] Rishabh Bailey, Smriti Parsheera, Faiza Rahman & Renuka Sane, "Disclosures in privacy policies: Does "notice and consent" work?", *National Institute of Public Finance and Policy,* December 11,2018, https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

[14] Malavika Raghavan, Anubutie Singh, "Building safe consumer data infrastructure in India: Account aggregators in the financial sector (Part 1)", *Tech law forum @NALSAR,* December 30, 2019 https://techlawforum.nalsar.ac.in/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector/

upon the Account Aggregator specified by the Reserve Bank of India as the consent manager model to be deployed in the fintech sector; which it proposes to be extended to other sectors as well. The Account Aggregators have been established by way of a notification issued by the Reserve Bank of India and is specific to the financial sector. Currently, there is no framework for the deployment of DEPA in other sectors, though the report does mention that the National Health Authority has been tasked with implementing the National Digital Health Mission, and is piloting the DEPA architecture for healthcare data. However, as mentioned earlier, no information has been provided as to the mechanism/architecture to be followed by the NHA for adopting a DEPA model based on the financial sector to the health sector. Similarly, the report does not provide any information /guidelines on the framework to be adopted by the other sectoral regulators.

We recommend that the framework and contours of DEPA should be established by way of a law passed by Parliament. The law should clearly stipulate the architecture of DEPA, its purpose, limitation on data collection, and grievance redressal mechanism. The sector specific granular details could be left to the sectoral regulators. It should also specify the relationship between this framework and the proposed Protection of Personal Data law.

7. **DEPA as a digital public good:** The promise of emerging digital public goods is immense[15] - and the DEPA is poised to become the building block of key public digital infrastructures in India. However, especially if it is going to function as a digital public good, it needs to adhere to the nature of a digital public good; and thus, be built in consonance with proper privacy protection, data governance frameworks, and incorporate necessary freedom from intellectual property laws.

   The 2020 Roadmap to Digital Cooperation by the UN Secretary General defines digital public goods as: "digital public goods must be open source software, open data, open AI models, open standards and open content that adhere to privacy and other applicable laws and best practices, do no harm, and help attain the SDGs."[16] Further, the recommendation on digital public goods said that a multi-stakeholder alliance, involving the UN should share and pool digital public goods and data sets, in a privacy-respecting way. At the very least, the compliance with the ingredients of 2020 Roadmap to Digital Cooperation should be ensured to claim that the DEPA is a (pure) digital public good. Presently, the DEPA is being implemented without an enacted data protection law in India, amidst other insufficiencies in terms of open source software, open AI models, and open content.

---

[15] Anita Guruswamy and Nandini Chami, "Digital Public Goods: A Precondition for Realising the SDGs", *Stiftung Entwicklung und Frieden,* 2019, https://www.sef-bonn.org/fileadmin/SEF-Dateiliste/04_Publikationen/GG-Spotlight/2019/ggs_2019-04_en.pdf

[16] United Nations, Secretary General Roadmap for Digital Cooperation https://www.un.org/en/content/digital-cooperation-roadmap/