# #NAMA: Issues with data localisation norms in the Personal Data Protection Bill, 2019

*The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focuses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.*

*Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.*

*The following is Part I of our notes from the session on cross border data flows, read Part II here.*

## Data localisation in the 2019 Bill: Not really an improvement

The data localisation norms under the current Bill are **not an improvement** over the Srikrishna Committee's draft bill, said a speaker.

**Segregation of data by type is very tricky**: "The datasets that we work with might be a mix of personal data, sensitive personal data, and maybe even critical personal data. But the data localisation or data mirroring requirement would be applicable to the whole data set, and it makes no sense for us to scrub and segregate personal data from it to send it outside India," the person added.

Mirroring of sensitive personal data in India would be challenging, because implementing mirroring standards and infrastructure would be difficult, another speaker said. The list of sensitive personal data includes things like caste, tribe, political inclinations and religious beliefs, and to extricate all such information from datasets would be a "nightmare," the person added. Illustrating the challenge in mirroring sensitive personal data, the speaker said: "Imagine a YouTube video where someone has commented about the Citizenship Amendment Act protests; that definitely is a political opinion, which would now have to be mirrored in India. It's an extremely difficult exercise".

- **Why even mirror?** If the data is about consumer protection, all transfers would have to be approved by the Data Protection Authority (DPA), businesses will be under strict contractual clauses by virtue of being part

of intra-group schemes, a person said. The person asked that if the transfer of sensitive personal data is going to be so heavily regulated, what is the need to mirror it in India in the first place?

**Enforcing segregation and localisation will be an issue:** Ensuring that data fiduciaries have localised relevant data would require for someone to look at how networks are designed, how data flows between data centres take place etc., the first speaker said. Highlighting the problems with enforcing data localisation, the speaker added, "you just have to say I have done it [data localisation], and here are three possible sources of evidence. But, in reality, there are maybe a hundred different ways in which data can still keep going outside the country because of how hard it is to perform localisation along with segregation".

- **The economics don't work:** There is also an economic element that might make enforcing data localisation a problem, several speakers concurred. "The most popular cloud service provider in the world lets people choose where they want their data to be processed and stored. If a user selects India to process their data, several services such as AI/ML, APIs are no longer available, and moreover, they will have to pay a price to perform the processing in India," a speaker said, highlighting the cost element behind data localisation.

**It's about government access:** The draft e-commerce policy had a protectionist intent, in a way that the concept of protecting Indians' data went beyond the idea of privacy. Similarly, the proposed changes to the intermediary guidelines, which require 24-hour communication with the government, show us that there is a regulatory intent for ensuring that Indians' data remains readily available and accessible to the government. That intent is going to find an expression through the data localisation norms in the current Bill, a lawyer explained.

**Seeking consent might be a problem for data processors:** While getting explicit consent can be easy for data fiduciaries, it becomes a problem for data processors who do not have a touch point with data subjects, a person explained. "As a data processor, when you are using the data for Big Data analytics, pattern generation, risk analysis, and don't have a touch point with data subjects, you will wonder if you can take data out India and combine it with other datasets to identify, for instance, frauds, terrorism risks," the speaker said.

**Good that personal data doesn't have to be localised:** All speakers concurred that the fact that personal data can be taken outside India was a welcome addition to the 2019 Bill.

**Food for thought: can users choose to store their data outside India?** "At a global tech summit, Justice Srikrishna was asked if citizens can exercise their right to privacy and ask for their data to be stored outside of India. He replied that he would have to go back and think about this," a speaker narrated.

## Data localisation is not about privacy or the economy

Given the types of data that have been categorised under sensitive personal data, such as financial data, it appears as if privacy has become a basic argument under which many other agendas get pushed through, a person noted. Privacy can not be a key argument for data localisation, they added.

**Is it about the economy then?** Several speakers concurred that data localisation's economic argument falls flat, simply because how can one leverage data stored within India, when the same data is also protected under a privacy law. "The economic argument often made in favour of data localisation is completely false, because you have a privacy regime, nobody is going to access the data to that end, since there is a purpose limitation, collection limitation and storage limitation. If I'm collecting and storing data in India, I'm not going to give it up since I have to also be compliant under the privacy law," a lawyer said.

- If it is about access to data, then storing the data in an encrypted form would defeat that purpose, another person said.

## How effective is seeking explicit consent?

Under the current Bill, sensitive personal data can only be processed outside India, and only with the explicit consent of data principals for such processing. But users may not be able to use all the features of a service, pointed out a speaker. In case a data subject doesn't give explicit consent, their sensitive personal information would not go outside the country; this would mean that the user will either not be able to use a particular service at all, or won't be able to use some features of certain products, a lawyer noted. "So, you won't be able to use some filters on Instagram because processing those filters on your photographs happens all over the world in disaggregated networks for speed. Because of that, you won't be able to use their products. So, you can use a minimal version of the service, but you can't use all the features that are actively available," the person illustrated.

> "If half the customers of a company were to give explicit consent to process their sensitive personal data outside India, and the other half did not, what will a business do? Are they supposed to have separate clouds to do the processing of data?" — a speaker asked

**Let data controllers do their due diligence:** Even the GDPR puts the burden on data controllers to have contractual provisions in place, and carry out their due diligence while taking people's data outside the European Union, a lawyer said. For the purpose of processing data outside of a particular border, the idea of seeking explicit consent from data subjects makes no sense at all, they held.

- Another speaker noted that it would be unfair to expect a data subject to decide what level of encryption should be applied to their data while consenting to process it outside India.

## Impact of data localisation on businesses

"Start-ups don't even know what's coming at them," a lawyer said, and added: "I was trying to log into a fitness app, and realised that they actually collect biometric data to mark attendance, and realised that they will have to now localise that data and segregate it from all other data sets they have". Another speaker said that the localisation norms can absolutely "disrupt" blockchain-based businesses and service.

- A lot of start-ups don't aim for monetisation from Day 1 of operations, and instead, use collected data to generate insights, customer onboarding and engagement in order to reach to a critical mass level, a person explained. The data localisation norms, thus, are more suited for bigger companies with tested revenue generation models since they will find it easier to comply with them, the speaker added.

**Need to re-engineer processes:** Both processing and classification of data from different datasets is going to be a painstaking exercise for several companies, a speaker noted. A lot of the companies have been operating under a free flow of data environment, and complying with the new norms would mean that they'll have to re-engineer a lot of their processes. This might result in a large number of companies to look for ways to keep all their data in India rather than take it outside, the person said, and added that it doesn't help that we are moving towards a heavily regulated environment where companies need to identify data starting from the collection itself, sort it, categorise it and then decide which data moves elsewhere.

**Fears of reciprocity:** While a lot of IT companies believe that the current localisation norms are slightly better than before, most of them have "expressed resistance" to the current rules because it puts barriers and they also fear that other countries might put similar barriers on them, a speaker said. "The IT industry fears that they could potentially lose out on international trade as a result," they added.

- IT service providers are also concerned about the intra-company transfer of data which has to be approved by the DPA, since it's going to be a major hassle, another person noted. They said that had the Bill allowed for a standard agreement with all clauses mentioned, it would have been much better.

**It affects B2B transactions as well:** "I started using Trello a few years ago, and I think I won't be able to use it anymore given that they will have to localise my payments data in India, which in all probability it wouldn't do given that it's a small company in San Francisco" an audience member noted. Similarly, small artisans, musicians, businesses would not be able to use cheap and good foreign tools because why would those companies want to invest in developing servers in India, the person said.

**Opportunity for larger players:** A speaker suggested how bigger companies

can potentially help smaller companies in complying with the localisation norms: "Companies like Apple can come up with a business model where anyone who wants to offer their services using their App Store can pay them an additional fee to purchase Apple's server space in India".

## What would be an ideal timeframe for data localisation?

**GDPR's two years wasn't enough:** "As of now, I can say that the two years allotted to comply with the GDPR was not enough," a speaker said. "Even for the companies who are already compliant to the GDPR may need more time, simply because our Bill is very different from the GDPR," they added. **When the GDPR came into force, it was found that almost 75% of the market was non-compliant**, a lawyer said. This, despite the EU having the Data Protection Directive in 1995, and the various judgements pronounced by the European Court of Justice. As of now, the apprehension is around not having clarity on when everything has to be in place, because when portions of the IT Act were enacted, we had seen how the government made radical changes without giving the market time to adjust to it, the person added.

> "Thinking of an adequate timeframe to comply with the localisation norms is a moot exercise, because even if you give companies a hundred years, they will not be able to meet the requirement. Unless they can prove that they have one dedicated data centre in India to comply with the norms, it will be difficult to be sure about it." — a lawyer

**Can data localisation norms be applied retroactively?** Businesses might have to seek fresh consent from data subjects to take their data out of India, despite the fact that they might have collected their data before the Bill was tabled, a lawyer explained.They will potentially have to do that because they could be using certain data for a completely different purpose than originally intended, they added.

## Recommendations

At least for sensitive personal data, the local storage requirement should be removed, and we can decide about localisation with respect to critical personal data on the basis of how it would be classified, a person said. Other recommendations made by speakers:

1. **Relax data transfer norms:** A lawyer said that If we can't remove data localisation from the Bill, we should ideally bat for relaxing some of the data transfer conditions, including not having to go to the DPA to get every transfer approved, another person remarked.
2. "All of the advanced data protection legislations in the world, including EU's GDPR, have no data localisation restrictions at all. They have restrictions on cross border data flows, and I think that's what we should

stick to," a lawyer noted.

3. Norms of data transfers in the Personal Data Protection Bill, 2019, are confusing and need to be relaxed.
4. **Focus on securing cross border transfers:** Restrictions on cross border data flow should be removed, localisation should be removed, and instead, we should focus on safe and secure transfer of data, be it through standards, standard contractual clauses, or adequacy.
5. **Sectoral regulations:** Instead of having a national law that dictates how localisation would work for everyone, we should leave it to the sectoral regulators to decide what works best for that particular sector.
6. **Need for a compliance roadmap:** The government should work responsibly and come out with a compliance roadmap, as was laid down in the previous version of the Bill, because without it, the situation would become chaotic.
7. **Explore global collaboration models** like the global privacy enforcement network (GPEN), so that countries respect each others' sovereignty while allowing for cross border data flows keeping rights of people in mind. Another user said that we can explore mutual recognition or bilateral agreements to allow for free flow of data outside India.

---

*Part II of our notes on cross-border data flow focuses on issues with classification of data, read it here. Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.*