Webinar Summary I Processing the DPDP Act:

Everything a Data Processor Must Know

The panel discussion featured insights from three experts: Supratim Chakraborty, Partner, Data Privacy and Protection Practice at Khaitan and Co, Kishore Mavuri, Data Protection Officer from Jio Haptik, and Ashok Hariharan, co-founder and CEO of IDfy. It was moderated by Niranjan Naragund, Privacy Consultant at IDfy.

Here are the key points discussed by each panellist:

Supratim Chakraborty
Khaitan & Co
Partner

Ashok Hariharan
IDfy
Chief Executive Officer

Kishore Mavuri
Jio, Haptik
Data Protection Officer

MODERATOR

Niranjan Naragund
IDfy
Privacy consultant

Supratim Chakraborty

Khaitan & Co

Partner

- Companies want to be branded as a controller or processor so they can have zero liability under the law. It is not about getting branded, but about the data processing taking place at the relevant journey level.

- The definition of a data processor is simple: Anyone who processes data on behalf of a fiduciary is a processor. It is a relationship of trust. We should keep this in mind at every level. As the ecosystem matures, we will see a common standard arrangement or ground elements of a contract. It won't matter if you are a controller or a processor – you will have to follow the law to protect the individual.

- Not every element of the DPDP Act would be granular enough in the rules. There may be certain parts that could need more detail. There may be certain other areas that shall be left to the industry to steward with responsibility. The reality is that we will be guided through mistakes and judicial precedents that get created.

- As sensitization increases and the law comes into force, there will be a spike in requests from data subjects alongside some random requests as well. It is important to really have a clearly laid out process with the data fiduciary because, ultimately, they are responsible.

- Data should be looked at from a harm-and-risk-based principle perspective. We should place backstopping – a holdback or bank guarantee – and other mechanisms, based on the contractual arrangement in question.

- Right now, a data processor might not have any liability, but it will eventually come via contractual obligations, making the situation even worse since it will be determined by the more powerful party. That determines who's making the other party really sign on the dotted line.

- Today, India does not have a threshold for anonymization. It is not called out very specifically in the law either. One way of looking at it is that the data is anonymized irreversibly, extricated from the natural person's identity and so on. But the way they're trying to look at it is that you can anonymize and utilize it, but with prior consent.

- There has been a widespread misconception about account aggregators becoming the automatic choice for consent managers but it is not so. Account aggregators, though following a consent mechanism, were conceptualized for entirely different reasons.

- There will be friction when a new law like the DPDP Act comes into play. We should try our best to see that innovation, entrepreneurship and ease of doing business are not hampered. It is an honest attempt. There would be certain friction but some of these could be teething issues. There will finally be a common standard from which the journey would be better.

Ashok Hariharan

IDfy

Chief Executive Officer

- There are real life examples to bear in mind: (a) The moment a payment gateway offers an option to create an easy check out the next time you visit, one has automatically moved into data fiduciary territory.
  (b) Notwithstanding a data processing agreement with Fiduciary 1, the moment data is stored, consent must be secured. The moment the data is used for an alternate purpose, one will be in breach of the agreement if they do so without taking consent. (c) When one buys data from data brokers, one is automatically a data fiduciary and has data from people whose consent they have not taken.

- At IDfy, we are very clear – one step of consent for each purpose for which the data is used.

- As a tech platform it's a lot easier to establish that you've deleted an artefact – as there is some provenance. How do you make sure that the ones who get these data delete it? That's where the problem really comes in. It's not just in the tech platform: It is a people-process-technology problem.

- The onus is on the fiduciary to audit their processes to make sure that there is conformity. The compliance responsibility for a fiduciary significantly increases. There's no answer in the pure tech world. There need to be regular audits to solve non-conformity.

- If processing takes seven days, you're likely archiving data every day to protect yourself. The moment you're done with processing, it becomes complicated if you have not thought about the data models you have in place to specifically delete those data points in your archive.

- Some level of standardisation will help processors comply with the DPDP Act, in line with data fiduciaries.

- While the law is the law and it might make it difficult for people to comply over the next couple of years, it is a good thing for the country and the citizens, because this law is not necessarily only to protect the fiduciary and the process, but also to protect the citizens.

- Account aggregators are not consent managers. Their scope is limited and does not account for various aspects of the DPDPA.

Kishore Mavuri

Jio, Haptik

Data Protection Officer

- Everybody has to comply with all the regulations, no matter who they are in the process.
- “Customer-facing” and “Non-customer facing” is one way of categorizing processors. Regardless, both process data on behalf of fiduciaries. For the end consumer, the fiduciary is the only one who is actually collecting or processing the data. They don't know who the processors are. This matters while taking consent.
- There are different sectors within any regulation. Each sector has its own obligations to fulfil. It is important to pay attention to the consent, responsibility, accountability, and ownership of the fiduciary rather than of the processor.
- Auditing should be part of the fiduciaries’ responsibilities. However, there are challenges for processors too. Sometimes, the end user may send a request for deletion directly to the processor. It is hard to identify to which customer the end user belongs. The responsibility to delete the data and communicate to the customer lies with the fiduciary. This is a tedious job, and the DPDP Act is not clear on this.

- As of now, the DPDP Act doesn't provide a timeline for compliance. As we see more and more people adopting it, we may get some clarity on industry standard practices. Right now, it is unclear. Eventually, everybody has to comply.

- The DPDP Act offers a technically infeasible requirement: For instance, in case of a data breach, each and every principal needs to be informed of this breach. A solution isn't readily available at the moment.

- We cannot conclude anything about the DPDP Act. We will have to wait for some time to gain some maturity once it is enacted.

- The real objective of the DPDP Act is that the beneficiaries are all residents of India. The government should educate all citizens. Once the awareness comes, we will see the real force of the law coming in.