Centre for Knowledge Sovereignty®

RECOMMENDATION FOR THE DIGITAL PERSONAL DATA PROTECTION BILL 2022

DEC 16, 2022

SUBMITTED TO <DHAWAL.GUPTA@MEITY.GOV.IN>, <NOTAN.ROY@MEITY.GOV.IN>

1. The bill does not cover the aspect of the storage of data, which may impact the data sovereignty of our nation. All the companies having operations in India and collecting personal data of Indians should store the data within the country. This will help LEA in accessing and retrieving data. Therefore, it is important to have a section for data storage.

2. 2(9) defines “gain” in a way that will put the “burden of proof on LEA” rather than the accused (in this case Data Fiduciary).

3. 2(10) should also consider “reputation loss”

4. The “offline personal data” mentioned in section 4(3)(b) should be defined in section 1. Offline personal data should not be excluded as it can be easily transmitted through electronic means. Such data can be processed in offline mode and the results can be published online.

5. In section 5, “deemed” should be removed as this will provide blanket permission to the Data Fiduciary and will often result in bypassing of the Data Principal.

6. The bill should clearly mention that the Data Protection Officer should be compulsorily posted in India and should be responsible for both the parent company as well as the Indian subsidiary.

7. The consequence of the withdrawal of permission by the Data Principal should be disclosed at the time of seeking consent. Otherwise, this will result in unlimited liability for the Data Principal. Any repercussion due to consent withdrawal should be proportionate and reciprocal in nature.

For example: In case of withdrawal of permission by the Data Principal, if there is a fine by the data fiduciary, then the user of data should also pay to data principal for using of the data. It should never bar the Data Principal from using the service.

1. The bill does not cover the aspect of the storage of data, which may impact the data sovereignty of our nation. All the companies having operations in India and collecting personal data of Indians should store the data within the country. This will help LEA in accessing and retrieving data. Therefore, it is important to have a section for data storage.

2. 2(9) defines “gain” in a way that will put the “burden of proof on LEA” rather than the accused (in this case Data Fiduciary).

3. 2(10) should also consider “reputation loss”

4. The “offline personal data” mentioned in section 4(3)(b) should be defined in section 1. Offline personal data should not be excluded as it can be easily transmitted through electronic means. Such data can be processed in offline mode and the results can be published online.

5. In section 5, “deemed” should be removed as this will provide blanket permission to the Data Fiduciary and will often result in bypassing of the Data Principal.

6. The bill should clearly mention that the Data Protection Officer should be compulsorily posted in India and should be responsible for both the parent company as well as the Indian subsidiary.

7. The consequence of the withdrawal of permission by the Data Principal should be disclosed at the time of seeking consent. Otherwise, this will result in unlimited liability for the Data Principal. Any repercussion due to consent withdrawal should be proportionate and reciprocal in nature.

For example: In case of withdrawal of permission by the Data Principal, if there is a fine by the data fiduciary, then the user of data should also pay to data principal for using of the data. It should never bar the Data Principal from using the service.

Centre for Knowledge Sovereignty®

https://www.linkedin.com/company/cksindia/

https://x.com/CKSIndia

https://www.youtube.com/@CKS_INDIA

www.cksindia.in