

Sansad TV Perspective: Digital Personal Data Protection Bill

In the series Sansad TV Perspective, we bring you an analysis of the discussion featured on the insightful programme 'Perspective' on Sansad TV, on various important topics affecting India and also the world. This analysis will help you immensely for the [IAS exam](#), especially the mains exam, where a well-rounded understanding of topics is a prerequisite for writing answers that fetch good marks.

In this article, we feature the discussion on the topic: '**Digital Personal Data Protection Bill**'.

Video link: <https://youtu.be/MVITck2h4fU>

Anchor: Teena Jha

Guests:

1. Khushbu Jain, Advocate, Cyber Security Laws
2. Amit Dubey, Data Technology Expert
3. Anuj Aggrawal, Chairman, Centre for Research on Cyber Crime and Cyber Law

Context: The draft Digital Personal Data Protection bill is out for public consultation.

Highlights of the discussion:

- Introduction
- Key provisions of the draft
- Challenges
- Way Ahead

Introduction:

- Three months after the withdrawal of the Digital Personal Data Protection Bill from [Lok Sabha](#), the government has come up with revamped legislation and sought views on it from the public.
- The draft is up for public consultation until 17th December 2022, and the final version is expected to be tabled in the Budget session of Parliament in 2023.
- The revised bill addresses several sticking points in the previous one which had been opposed by global tech companies and caused an industry pushback.
- The purpose of the legislation, as mentioned in the draft, is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes.

For more information on the Personal Data Protection Bill (2019), read here: [Personal Data Protection Bill, 2019.](#)

Key provisions of the draft Digital Personal Data Protection Bill:

- This is a shorter and simpler draft with nearly 30 to 34 provisions in contrast to the earlier bill which had hundred-plus provisions.
- The focus has clearly shifted to individual personal data and it has been defined very clearly. The rights of individuals and the obligation of the data processors are the two major objectives.
- A very important improvement of the draft regarding children's data. It is clearly highlighted that the guardians of the children would have to provide verifiable data about their children and would be responsible for their data.
- The right to portability that was provided in the previous version has been done away with.
- The 'deemed consent' has been introduced to cover non-consent-based grounds for processing data.
- Exemptions to certain central agencies are retained in contrast to the earlier provision of exemption to 'all' government agencies. Moreover, these exemptions have to be notified.
- There is recognition of [alternate dispute resolution](#) processes like arbitration.
- The new draft has watered down the local data storage requirements. But the transfer of data outside India is still limited. Moreover, the government will notify the countries where the data can travel.
- A sharp focus has been given to regulating personal data. Moreover, it does not cover aspects like non-personal data (which existed in the last amendment of the previous bill).
- Hardware certification and algorithmic accountability are also eliminated in the new proposal.
- For probably the first time any draft has made the data provider responsible for the accuracy of data.
- The draft has also pointed to the duties and responsibilities of the citizens in protecting their data.
- The concerns raised by the industry, particularly startups in the previous bill have been addressed. There are certain relaxations provided to them.
- For the benefit of end users, a sort of deterrent has been provided for data leakages by imposing high penalties in case of a breach.
- Moreover, there is also a provision of consent for data sharing and only when permission is given by the end user, the data can be written.
- The personal identifiable data cannot be kept/stored for very long and there will be a time limit for such storage and in case of a breach, the organization can be penalized.
- Data redundancy will be reduced and eventually eliminated and data would be made more secure.

- The end users will also be guarded against social media and financial fraud in the cyber world.
- This is a friendly act as it provides a platform for Indian startups to innovate and flourish.
- Furthermore, no strict procedure has been put in place and just a framework is provided. The organization/company has the freedom to devise a procedure by imbibing the principle of data security.

Penalty Aspect of the Draft Digital Data Protection Bill:

- This is the area that is attracting multiple concerns from experts since its release.
- The earlier bill had the provision of a penalty of 4% of the global turnover per breach and in case of non-compliance, the penalty was 2% of the global turnover. This was a high penalty. However, it was proportionate as the small companies will have lower turnovers.
- This provision has been changed to 'up to 500 Crores'. It will again be a proportionate system depending on the level and kind of breach. This will be ascertained by an authority like a data protection board.
- This sort of provision is particularly good for Indian startups and industries. However, when it comes to tech giants like Google and Twitter, the amount of 500 Crore is very less.
- If the companies can justify that the data was managed well with all security procedures and auditing schemes in place, then a penalty might not be imposed.

Associated challenges with the draft:

- The nature of the Data Protection Board is still not clear. It should be clarified whether it would be a judicial body or an administrative body.
- If [data localization](#) is not strictly imposed there is a threat of data being weaponized against the country.
- There are also concerns about the wide-ranging exemptions provided to the Centre and its agencies.
- It is also apprehended that there is a reduction in the independence of the proposed regulator.
- Several experts also suggest that changes cannot be expected by just putting the guidelines. There should be clear and instant procedures for penalizing a breach in security.
- The draft will solve the issue of data security only in the primary stage and lacks provision for advanced and complex cases.
- Another challenge associated is the emergence of the metaverse and its probability to impact every aspect of life.
- A single framework for different sectors like [e-commerce](#) platforms, health techs, automobile companies, etc. is also a serious concern.

Way Ahead:

- There should be a graded system of penalties with the right checks and balances.
- The penalty should be linked to the number of subscribers and the kind of data.
 - For instance, each and every personal data adds approximately \$150 to an enterprise.
 - It should also be noted that India is one of the largest sources of such data and supplies wholesale data to big tech companies abroad.
 - This data is further used to build high-tech technologies based on machine learning and artificial intelligence and add huge profits for foreign companies.
- The companies also need to be graded based on their size, location, and data utility. For example, if the companies help strengthen the Indian ecosystem of artificial intelligence or machine learning then some leeway can be provided to them.
- Lessons can be learned from the Californian law that has very clearly prescribed the rules and regulations.
- There should be different layers and standards for different domains like health, education, e-commerce, social media, etc.
- The new laws should be clearly enforceable and properly implemented to reap the maximum benefits.
- There is a scope for improvement in the localization aspect which should be resolved.