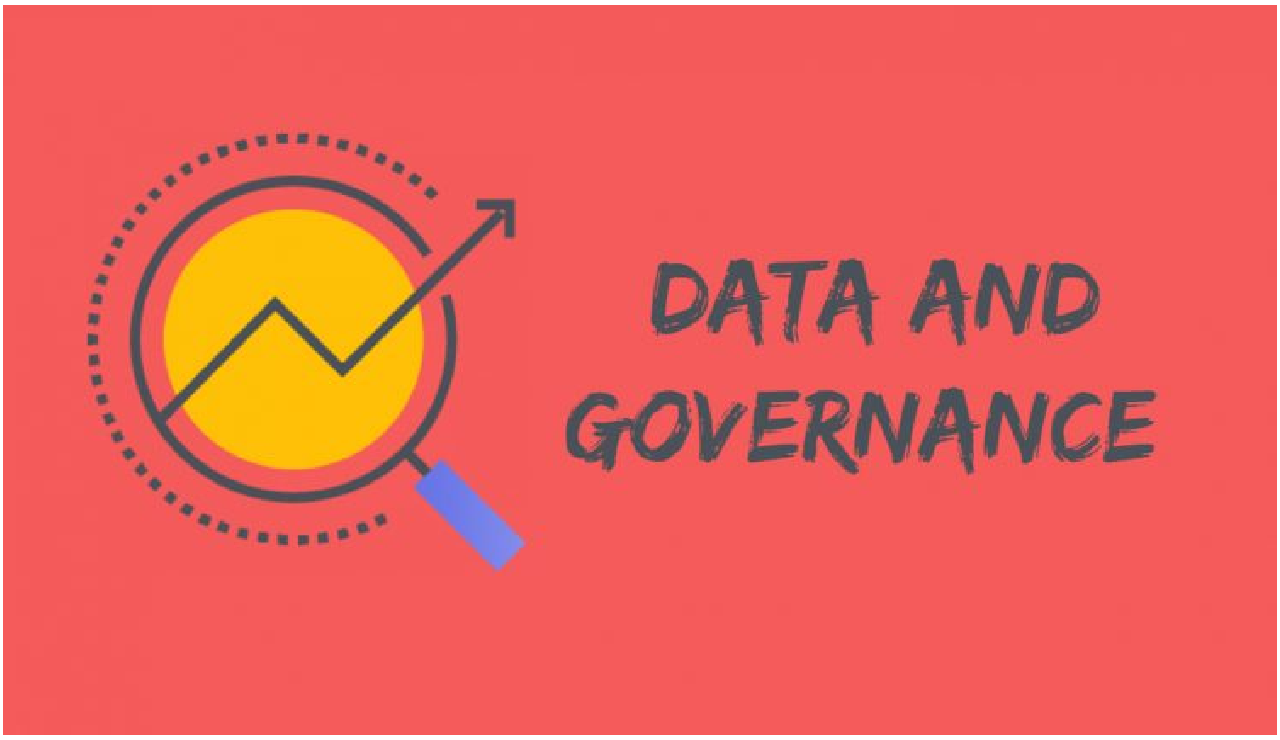
Data and Governance | New Topic in UGC NET EXAM

ugcnetpaper1.com/data-and-governance/

March 10, 2020



Data and Governance

The 21st century has witnessed such an explosive rise in the number of ways in which we use information, that it is widely referred to as ‘the information age’. It is believed that by 2020, the global volume of digital data we create is expected to reach 44 zettabytes.

Much of that new information will consist of personal details relating to individuals, including information relating to the products they have purchased, the places they have travelled to and data which is produced from ‘smart devices’ connected to the Internet.

Use of social media networks such as Facebook & WhatsApp produces a large amount of data every day some of which contains personal information.

There are a large number of benefits to be gained by collecting and analyzing personal data from individuals. Both the public and the private sector are collecting and using personal data at an unprecedented scale and for multifarious purposes. While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of an individual.

Not only this Facebook was in news for platform personal data uses without consent and later Facebook was forced to update the data policy to strengthen the data privacy checks.

Data and Governance.

- Data governance is primarily used to refer to the strategy of managing and controlling data.
- Data governance is the overall management of data availability, relevancy, usability, integrity and security
- The drivers of data governance are usually regulatory and legal requirements; however, a governance rule can be any practice to which the organization wishes to adhere.
- Governance often dictates where certain types of data may be stored and codifies data protection methods, such as encryption or password strength.
- Governance can dictate how to back up data, who has access to data, and when archived data should be destroyed.

What is the benefit of data governances?

In 2017 that the Ministry of Electronics and Information Technology released a White Paper by a committee of experts led by former Supreme Court judge, Justice B.N. Srikrishna, on a data protection framework for India.

The committee identified seven key principles for the data protection law:

- Technology agnostics
- Holistic application
- Informed consent
- Data minimization
- Controller accountability
- Structured enforcement
- Deterrent penalties
- Protection of sensitive personal data

It envisions three main objectives of a data protection authority: monitor, investigate and enforce the laws; set the standards; and generate awareness in an increasingly digitized society

What is data governance & General data protection laws framework in India?

Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize intrusion into one’s privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency.

Related Posts

Sources acquisition and classification of Data

Solving Tricks | Data Interpretation NET EXAM | Updated 2020

The Government has notified the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.* The Rules only deals with protection of "Sensitive personal data or information of a person", which includes such personal information which consists of information relating to:-

- Passwords;
- Financial information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information.

The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with "Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of the body corporate, the body corporate may be held liable to pay damages to the person so affected.

- India is not a party to any convention on the protection of personal data which is equivalent to the GDPR or the Data Protection Directive.
- Indian legislature did amend the Information Technology Act (2000) ("IT Act") to include Section 43A and Section 72A, which give a right to compensation for improper disclosure of personal information.
- The Indian central government subsequently issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Rules") under Section 43A of the IT Act.
- The Ministry of Electronics and Information Technology (the "Ministry") is responsible for administering the IT Act and issuing the rules and other clarifications under the IT Act.

Under section 72A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000 (approx. US$ 8,000).

Sensitive personal data

Sensitive personal data exists as the concept of sensitive personal data or information under the Rules. It means personal information which consists of: (i) passwords; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above items provided to a body corporate for providing services; and (viii) any of the information received under above items by a body corporate for processing, that is stored or processed under lawful contract or otherwise.

Sensitive personal data or information does not include information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other applicable law.

Open data

Open data is the idea that some data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control. This concept tailed governing doctrine termed as open government.

Open government gives right to the citizens to access the documents & proceedings of the government to allow for effective public oversight. The blend of these two concepts give rise to Open Government Data (OGD) or data-driven governance.

Open Government Data promotes transparency, accountability and value creation by making government data available to all. In India Open Government Data(OGD) platform can be experienced on www.data.gov.in. It is the reservoir of all the open government data.

Benefits:

- Increases Transparency and Accountability: Members of the public can stay connected, informed, and up to date with the day-to-day operations of their local government. The public nature of this information holds governments accountable to the results they produce. E.g. e-RTI
- Develops Trust, Credibility and Reputation: The transparent nature of publicly accessible data exposes a side of an organization which is quite often kept under wraps.
- Promotes Progress and Innovation: Third parties without the resources to gather this data for themselves will be able to re-purpose it and utilize the information to develop new applications and services. E.g. Drought Data helped to analyze the reasons & solutions to it.

- Encourages Public Education and Community Engagement: What better way to educate the community on the progress and performance of the city than to have all the information displayed in a clear and user-friendly display? Access to meaningful data aids in unifying a community and empowering them to help shape the direction for the future. E.g. www.community.data.gov.infor common platform for knowledge sharing through discussion and to contribute through Blogs, Info-graphics, Visualizations, etc. using data available on the platform.
- Stores and Preserves Information Over Time: The availability of consolidated information in a single and easily accessible location is advantageous for the use of both current information and for historical data that has been gathered over time. E.g. Health Record

Challenges:

1. Lack of Infrastructure: The entire infrastructure of information gathering, processing, sharing is to be found wanting.
2. Insufficient Standardization
3. Issue of Semantic Interoperability—e.g., different departments gathering different information under the same heading or the same information under different headings—that can’t be tackled as easily.
4. Issues of privacy are importantly implicated, especially since there is no written law on privacy in India, and data anonymization is seldom practised.

To ensure the relevance of open government data, mechanisms have to be put in place to take its benefit to the common person and to marginalised communities, both by the government as well as by civil society organizations; putting up raw data will not suffice.