GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1846
TO BE ANSWERED ON: 04.08.2023

DATA PROTECTION AUDIT OF TECH COMPANIES

1846. SHRI RAJMANI PATEL
SHRI NARANBHAI J. RATHWA:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) Government's plan for data protection audit of big tech companies;

(b) whether it is a fact that foreign companies like Walmart, Google, Amazon, Facebook and Flipkart are taking control of Indian financial data which will set a precarious precedence in future; and

(c) if so, the steps being contemplated by Government for imposing tighter regulations on such foreign players on data protection?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users.

As introduced on 3rd August, 2023 the Digital Personal Data Protection Bill (DPDP), 2023 can protect the rights and prevent the misuse/exploitation of the personal data of the Digital Nagriks while bestowing the obligations on the data fiduciaries. The proposed bill is expected to create deep behavioral changes in the current practices among some big tech platforms/data fiduciaries to prevent misuse and exploitation of the digital personal data of Digital Nagriks of India. The Bill proposes to create a framework to protect the rights of Indian Digital Nagriks and prevent such misuse of their personal data.

For significant data fiduciary it is envisaged in the Bill that a higher threshold of oversight and regulation are prescribed including but not limited to the audit.

(b) and (c) The provisions of the DPDP, 2023 Bill ensures that no platform also known as data fiduciaries will be able to misuse or exploit the personal data of Indian Digital Nagriks.

Leading to the enactment of the Digital Personal Data Protection, Bill, 2023 the Government and citizen rely on the Information Technology Act, 2000 and the Rules made thereunder.

Section 43A of the Information Technology Act, 2000 provides that a body corporate which possesses or deals or handles any sensitive personal data or information in a computer resource owned or controlled or operated by it is liable to compensate an affected person for causing wrongful loss or wrongful gain to any person due to negligence in implementing and maintaining reasonable security practices and procedures. Government, in exercise of its powers under the said section, has prescribed the rules regarding sensitive personal data

or information as well as the reasonable security practices and procedures to be complied with.

Also, to protect personal data of users, the Central Government, in exercise of its powers under the Information Technology Act, 2000, has prescribed reasonable security practices and procedures and sensitive personal data or information through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Under these Rules, the body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified shall be deemed to have complied with reasonable security practice and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

Additionally, National Payment Corporation of India has been directed to conduct or get conducted audits, including system and governance audits as well as assessment of compliance of provisions of various laws, rules and regulations, UPI procedural guidelines, circulars / instructions issued by NPCI / RBI and other regulators, of systems and underlying infrastructure / network / applications related to UPI for each of the Third Party Application Providers (TPAPs) (such as Google Pay, PhonePe, Amazon Pay, Whatsapp Pay, etc.) at least on annual basis, insofar as they relate to Third-party Application Providers (TPAPs) operating on multi-bank model. For all other TPAPs, the same shall be conducted at least on bi-annual basis. The scope of audit includes compliance with RBI's instructions on data storage.

Reserve Bank of India has issued a directive (under Sections 10(2) and 18 of the Payment and Settlement Systems Act 2007), vide circular DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 06, 2018 on 'Storage of Payment System Data' advising all system providers to ensure that, the entire data relating to payment systems operated by them is stored in a system only in India.

Also, RBI has published FAQs in this regard, on June 26, 2019, to provide clarity on certain implementation issues to facilitate and ensure expeditious compliance by all Payment System Operators.

****