As introduced in the Rajya Sabha
on the 5th August, 2016

Bill No. XXIII of 2016

THE RIGHT TO PRIVACY OF PERSONAL DATA BILL, 2016

A

BILL

to provide for the right to privacy of personal data to all individuals in the country, establishing the liability of the organizations as well as the appropriate Government in case of misuse of such personal data of individuals, for creation of a National Do-Not-Disturb Registry to ensure that individuals are not harassed by organisations and creating awareness among individuals for protection of their personal data and for matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Sixty-seventh Year of the Republic of India as follows:—

Short title, extent and commencement.

1. *(1)* This Act may be called the Right to Privacy of Personal Data Act, 2016.

(*2*) It extends to whole of India.

(*3*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

Definitions.

2. In this Act, unless the context otherwise requires,—

(*a*) "appropriate Government" means in the case of a State, the Government of that State and in all other cases, the Central Government;

(*b*) "business contact information" means and includes individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by individual solely for his personal purposes;

(*c*) "data subject" means an individual whose personal data is being processed;

(*d*) "individual" means a human being whether living or deceased;

(*e*) "intermediary" means an organisation which processes personal data on behalf of another organisation;

(*f*) "national interest" includes issues of national security, defence and conduct of international affairs;

(*g*) "organisation" includes any individual, company, intermediaries, contractors, association or body of persons, corporate or unincorporated,whether or not—

(*i*) formed or recognised under any law of the country; or

(*ii*) resident, or having registered office or a place of business in India.

Explanation.— Organisation shall also include Government Ministries, Departments and public funded Institutions at all levels.

(*h*) "personal data" means any data, whether true or not, about an individual who can be identified from that data and other information about an individual which any organisation has collected or is likely to have access to;

(*i*) "prescribed' means prescribed by rules made under this Act;

(*j*) "privacy risk" means the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional or any other harm to an individual;

(*k*) "processing of personal data" means taking any action regarding data that is linked to an individual or a specific device, including but not limited to collecting, retaining, disclosing, using, merging, linking, and combining data.

Right to Privacy of Personal Data.

3. (*1*) Every individual, whether he is citizen or not, shall have the right to privacy of personal data generated by him while staying legally within the country.

(*2*) Notwithstanding anything contained in any other law for the time being in force, no person shall process the personal data without the consent of the individual:

Provided that if the individual is deceased, after the commencement of the Act, this right shall pass on to his legal heir(s), as the case may be.

(*3*) Before taking the consent for processing of personal data every organisation shall provide the individual in concise and easily understandable language, accurate, clear, timely and conspicuous notice of its privacy and security practices.

(*4*) Every organisation shall provide convenient and reasonable access to such notice, in electronic, physical or any other feasible form, and any updates or modifications to such notice to the individual whose personal data is processed.

(*5*) **After taking the consent, every organisation shall provide the individual with reasonable means to control the processing of personal data in proportion to the privacy risk to the individual.**

Creation of a National Do-Not-Disturb Registry.

4. (*1*) The appropriate Government shall create a Registry to be named as National Do-Not-Disturb Registry where individuals living in the country can register themselves to restrict any sort of communication, in any form including but not restricted to receiving phone calls, messages, or mails.

(*2*) The appropriate Government shall take necessary measures to promote the National Do-Not-Disturb Registry and make the individuals aware of the same.

Creation and review of data requirement policy.

5. (*1*) All organisations shall create a data requirement policy, within three months of the commencement of the Act, and shall review the actual requirement of personal data of individuals on a peridical basis.

(*2*) The review of data requirement policy shall be updated on a yearly basis unless a need to update the same arises earlier for an organisation.

Creation of awareness of protection of personal data.

6. The appropriate Government shall take necessary measures for creation of awareness of protection of personal data among the persons living in the country.

Restrictions on right to privacy of personal data.

7. Notwithstanding anything contained in this Act, the right to privacy of personal data of the individual shall be restricted,—

(*a*) for matters of national security;

(*b*) to protect the life and health of an individual who is not able to express his consent;

(*c*) for the data of the individuals, deceased before the commencement of the Act;

(*d*) when an individual is acting in the course of his employment with an organisation; and

(*e*) for business contact information.

Guidelines for privacy of personal data.

8. (*1*) The appropriate Government, as and when required, shall issue guidelines for maintaining privacy of personal data.

(*2*) The guidelines shall be issued after due consultations with the concerned stakeholders.

Coordination within appropriate Government.

9. The appropriate Government shall take all measures to ensure effective coordination between services provided by concerned Ministries and Departments such as those dealing with Law, Home Affairs, Human Resource Development, Information and Technology, Information and Broadcasting, Defence, Corporate Affairs and External Affairs to address issues of privacy of personal data.

Establishment of National Research Centre for Excellence in Data Management.

10. (*1*) The Central Government may, by notification, establish for the purposes of this Act, a National Research Centre for Excellence in Data Management which shall conduct holistic research activities in the field of data management.

(*2*) The Central Government may, by notification, specify the headquarters of the Research Centre established by it under sub-section (*1*).

(*3*) The salary and allowances payable to and other terms and conditions of the officers and members of staff of the Research Centre shall be such as may be prescribed.

Compulsory education of privacy of personal data in educational institutions.

11. (*1*) On and from such date, as the appropriate Government may, by notification in the Official Gazette specify, the education of privacy of personal data in educational institutions shall be imparted compulsorily from such class onwards as may be prescribed by the appropriate Government.

(*2*) Subject to such rules, as may be prescribed, the appropriate Government shall

ensure appointment of such number of teachers with such qualifications, as may be specified, for teaching privacy of personal data in educational institutions.

Public Servants not to misuse access to personal data of citizens.

12. No public servant shall misuse the access to personal data or track the personal data of the individiual including the Members of Parliament, Members of Legislative Assembly or Council except for matters of national security.

Central Govenment to provide funds.

13. The Central Government shall, after due appropriation made by Parliament by law in this behalf, provide requisite funds for carrying out the purposes of this Act.

Penalty.

14. (*1*) Any organisation who directly or indirectly contravenes or attempts to contravene the provisions of this Act, shall be punished with imprisonment for a term which may extend to seven years or with fine up to fifty lakh rupees or with both.

(*2*) The penal provisions shall not apply to the individuals including the directors of the organisations who can prove their innocence with regard to the illegal data processing conducted in the organisation.

Payment of financial compensation to aggrieved individuals.

15. In cases where it is proved that the organisation has undertaken illegal personal data processing of individuals, the organisation shall be liable to pay ten times the revenues earned from such activities as compensation to the aggrieved individuals.

(*2*) In case the organisation is unable to pay such financial compensation, their assets shall be liable to be attached for this purpose.

Power to remove difficulties.

16. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act, as appear to it to be necessary or expedient for removing the difficulty :

Provided that no such order shall be made after the expiry of the period of three years from the date of commencement of this Act.

Act to have overriding effect.

17. The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law the time being in force.

Power to make rules.

18. The Central Government may, by notification in the Official Gazette make rules for carrying out the purposes of this Act.

STATEMENT OF OBJECTS AND REASONS

Personal data refers to data, whether true or not, about an individual who can be identified from that data and other information to which any organisation has or is likely to have access. In the earlier times, personal data of citizens was confined to limited domains of Government records and paper documentation managed privately by citizens. However, India has witnessed a digital revolution at the cusp of the 21st century. The social and economic landscape of the country underwent a metamorphosis with the advent of technology. With this, the scope of personal data expounded exponentially. *According to data industry giant IBM website, nearly 90% of the total data in the world has been created in last two years alone.* A major portion of this personal data is generated through electronic medium chiefly through the means of internet. With the advent of cloud compouting, millions of terabytes of data get uploaded on the web on a daily basis.

In the past two decades, there has been a meteoric rise in promoting digital governance in the country and the same has been undertaken in the recent months under the Digital India Initiative. Digital provisions of governmental, banking and various other necessary services have given way to generation of millions of terabytes of sensitive citizen data in the country. There has been an upsurge in the use of e-Locker services (DigiLocker) provided by the Government and various cloud based storage applications for storing crucial personal data by the citizens. The marquee government program for digital identification of all its citizens (Aadhaar) is on its way of completing a universal coverage in the country.

With an array of governmental services being provided digitally to the citizens, there lies an imminent threat of unauthoried capturing and recording of personal data generated through the provisions of these services. With the meteoric rise of the Business Process Outsourcing (BPO) industry in the country, the demand for personal data of people is huge and in order to cater to the same, there has been a rise of a *data mafia* and an entire illegal industry has come up, worth thousands of crores which would provide personal details of citizens for profit-making purposes. Due to phenomenal penetration of smartphones in the country, there has been a rise in the application (Mobile App) culture and data generated on these applications has also increased significantly.

In such circumstances, it becomes extremely important to protect the personal data especially generated through electonic means belonging to the citizens in the country. Individual data of extremely sensitive nature such as retina scans, thumb imprints of millions of Indian citizens collected under Aadhaar need highest degree of safeguards especially when the same is collected by private Enrolment Agencies. The data captured under e-Locker and online storage programs need comprehensive security considering the invaluable nature of data stored in the same by the Indian citizens.

There is also an urgent need to create a broad, transparent and comprehensive framework to determine the liability of the organizations collecting, storing and maintaining the personal data of the user. There is a need to introduce a 'Review of Data Requirement Policy' to keep a check on the greed of organizations seeking more data for nefarious purposes. This policy must specifically differentiate the instances where the need is of mere identification of individuals and cases where specific personal data of the citizens is required. Despite having a Do-Not-Disturb (DND) Policy in place, the organizations have found loopholes within the same and the tele-marketing harassment of common and innocent citizens in the country continues. There is a need to legislate for the creation of a National Do-Not-Disturb Registry (NDNDR) along with stringent penal provisions against the organizations which harass the citizens who register their numbers within this Registry. There is also an urgent nned to create awareness among the citizens to explain the significance of their personal data and the need to protect the same. A large number of instances have come to light where the

access to personal data of the politicians in the country especially the Parliamentarians at both the central and state level is misused for political vendetta. Hence, there is a need to bring the Government officials to be brought under the purview of the Act in order to ensure that such illicit tracking and misuse of access to personal data can be prevented.

Various countries across the globe have recognized the importance of enacted comprehensive legislations giving protection to data of its citizens.

Various provisions in the current legal framework including the information Technology Act deal with the protection of data of the citizens. However, the laws in this country have not been able to keep up with the speed of fast changes occurring in the world of technology. There is a need to make the penal provisions for illegal capturing, storing and performing other such malicious activities with the personal data of the citizens even more stringent. There is also a need to introduce a component of payment of financial compensation to aggrieved user whose data has been misused by the organizations in order to disincentivize perfomance of such unlawful activities.

Hence, in the times when the internet and data generated through the same are becoming ubiquitous, it is pertinent that the rights in relation to the same are imparted to the citizens and such a measure will surely help in proving the age old adage *'A stitch in time, saves nine.'* The AP shah Committee submitted a report on the need to enact a law on privacy in the year 2012. Despite the passage of four years, still the Government has not enacted a comprehensive law on data privacy in the country. *It is high time that a law should be enected to protect the very foundational premise for the success of Digital India which is the protection of data of its citizens without further delay.*

The need of the hour is to develop fool-proof data-protection laws in the country. There is an urgency to create a comprehensive law for imparting holistic privacy to the personal data of the citizens of this country.

Hence, this Bill.

VIVEK GUPTA

FINANCIAL MEMORANDUM

Clause 4 provides for creations of a National Do-Not-Distrub Registry. Clause 6 provides for creation of awareness of protection of personal data. Clause 10 seeks to establish a National Research Center for Excellence in Data Management. Clause 13 provides that the Central Government shall provide requisite funds for carrying out the purposes of the Bill. At this stage, it is not possible to estimate the amount to be incurred. However, the Bill, therefore, if enacted, will involve expenditure from the Consolidated Fund of India. It is estimated that an annual recurring expenditure of about rupees one thousand crore would be involved.

A non-recurring expenditure of rupees one thousand and five hundred crore is also likely to be involved.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 18 empowers the Central Government to make rules for carrying out the purposes of the Bill. As the rules will relate to matters of details only, the delegation of legislative power is of a normal character.

RAJYA SABHA

A

BILL

to provide for the right to privacy of personal data to all individuals in the country, establishing the liability of the organizations as well as the appropriate Government in case of misuse of such personal data of individuals, for creation of a National Do-Not-Disturb Registry to ensure that individuals are not harassed by organisations and creating awareness among individuals for protection of their personal data and for matters connected therewith or incidental thereto.

(Shri Vivek Gupta, M.P.)

GMGIPMRND—2238(S3)—05.08.2016.