GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *250
TO BE ANSWERED ON: 02.08.2017

REGULATORY REGIME/POLICY FOR DATA PROTECTION

***250 SHRI CH. MALLA REDDY:**
SHRI HUKUM SINGH:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether the Government proposes to bring in a new regulatory regime and/or any policy for data protection, if so, the details thereof and the time by which the said regime/policy is likely to be operational;

(b) whether the data pertaining to subscribers of a private company was allegedly leaked/breached on an independent website, if so, the details thereof and the reaction of the Government thereto;

(c) whether the Government has sought details of the said incident from the aforementioned company;

(d) if so, the details thereof along with the steps taken by the Government in this regard; and

(e) the other steps taken by the Government to curb such breaches/leakages of subscribers' data?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a) to (e): A Statement is laid on the Table of the House.

STATEMENT REFERED TO IN REPLY TO LOK SABHA STARRED QUESTION *250 FOR 02.08.2017 REGARDING REGULATORYREGIME / POLICY FOR DATA PROTECTION.

……..

(a): Ministry of Electronics and Information Technology (MeitY)has recently been mandated to develop a Framework for Data Protection Law for protection of online personal data. The modalities and timelines are being worked out.

(b),(c) and (d): It was reported that data pertaining to subscribers of a private telecom company was available through a website on 09th July 2017. It was reported that on entering a subscriber mobile number on this website, it would sporadically return the name, mobile number, email-id, SIM card activation date and Circle code. Aadhaar number was however not available through this method. The concerned company has lodged a complaint and FIR with Navi Mumbai Police and reported the incident immediately to Department of Telecommunications (DoT), Indian Computer Emergency Response Team (CERT-In), and National Critical Information Infrastructure Protection Center (NCIIPC).The said website became inoperational on 09thJuly 2017 itself. CERT-In has sent an advisory to the concerned company on 10th July 2017 mentioning the immediate actions to be taken to enhance the security of its networks and services. DoT has also instructed them to take corrective action to prevent such incidents in the future. Moreover, other Telecom Service Providers have also been instructed to examine their systems and take necessary corrective action.

(e): Department of Telecommunications (DoT) has already mandated all the Telecom Service Providers (TSPs) who have been granted license under section 4 of the Indian Telegraph Act 1885 to protect the privacy, confidentially and security of information as has been stated in clauses 37.1, 37.2, 37.4, 39.4, 39.23 in the telecom licence agreement. TSPs have also been mandated to create facilities for monitoring all intrusions, attacks and frauds and report the same to the DoT and to Indian Computer Emergency Response team (CERT-In). They are required to audit their network or get the network audited from security point of view once a year from a network audit and certification agency. DoT also conducts Security Audit to ensure implementation of security policies in the Telecom Service Provider networks.

In addition, the Information Technology Act 2000 is also applicable to TSPs and they are also required to implement reasonable security practices and procedures to protect the information.

CERT-In has also empanelled auditors to facilitate body corporates to audit their information technology infrastructure and implementation of security best practices.

****