

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**RAJYA SABHA**  
**UNSTARRED QUESTION NO. 737**  
TO BE ANSWERED ON: 8.12.2023

**BREACHES OF INDIAN CITIZENS' DATA**

**737. SHRI SAKET GOKHALE:**

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

- (a) the total number of data breaches of Indian citizens' that have been brought to the notice of the Ministry since January 2018;
- (b) the specific instances or cases of data breaches of Indian citizens' currently being investigated by the Ministry or law enforcement agencies;
- (c) the total number of breaches of COWIN data & Aadhaar (UID) data reported to the Ministry; and
- (d) the specific actions taken by the Ministry to address COWIN & Aadhaar data breaches?

**ANSWER**

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

(a) to (d): The policies of the Government are aimed at ensuring an open, safe, trusted and accountable internet for its users. Government is fully cognizant and aware of various cyber security threats and challenges and has taken various measures to prevent cyber-attacks/breaches to ensure data safety of the citizens. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 165 data breach incidents involving citizen data are observed from January 2018 till October 2023. No breach of Aadhaar card holders' data has occurred from the Central Identities Data Repository (CIDR) maintained by the Unique Identification Authority of India. To ensure safety of the personal and biometric data of the citizens on the Co-IN App/Portal, Ministry of Health and family Welfare(MoHFW)has taken several measures including ensuring:

- (i) Beneficiary can access vaccination details by registered mobile number through OTPauthentication only.
- (ii) Mobile Numbers, Aadhaar Number & other Photo ID Card numbers of beneficiary are masked. Only last 4 characters are visible to users (service providers) of Co-WIN.
- (iii) Complete Co-WIN database is encrypted using "Encryption Algorithm" key to protect citizen data and data integrity is maintained for all vital information.
- (iv) Two factor authentication feature (Password & OTP) while login by the users (service providers) is put in place restricting unauthorised access to Co-WIN

\*\*\*\*\*