GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**RAJYA SABHA**
**UNSTARRED QUESTION NO. 4589**
TO BE ANSWERED ON 06-04-2018

## INCIDENTS OF BREACH OF AADHAAR DATA

**4589. SHRI DEREK O' BRIEN:**

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

(a) the number and the details of incidents/cases where Aadhaar data was leaked/breached;
(b) whether any investigation has been conducted against the agencies which were responsible for breach/leakage of Aadhaar data;
(c) if so; the details thereof alongwith the action taken against them;
(d) the extent to which the database of Aadhaar is secured along with the steps taken by Government to ensure the privacy/security of Aadhaar data; and
(e) the mechanism put in place for usage of Aadhaar Data by the Government agencies and the accountability of officials in case of negligence on their part in handling of such data?

## ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS)

(a): As on date, no incident of data breach has been reported from Central Identities Data Repository (CIDR) of Unique Identification Authority of India (UIDAI).

(b) and (c): Do not arise in view of (a) above.

(d): UIDAI has a well-designed, multi-layered robust security system in place and the same is being constantly upgraded to maintain the highest level of data security and integrity. UIDAI has adequate legal, organizational and technological measures in place for the security of the data stored with UIDAI. Data Protection measures have also been mandated for the requesting entities and ecosystem partners to ensure the security of data. Government is fully alive to the need to maintain highest level of data security, privacy and is deploying the necessary technology and infrastructure. The architecture of Aadhaar ecosystem has been designed to ensure non-duplication, data integrity and other related management aspects of security & privacy in Aadhaar database. Additionally, various policies and procedures have been defined clearly which are reviewed and updated periodically, thereby, appropriately controlling and monitoring security of data. Some of the security measures adopted by UIDAI are as under:

- Information security policy has been established based on the ISO 27001:2013 standard. The policy covers all areas of Information Security such as Organization of

Information Security, Asset management, Access control, Technical vulnerability management, Change management, Patch management, Encryption, Service continuity, Operations security, Communications security, Supplier security, Human resources security etc.

- Chief Information Security officer has been appointed to drive Information security measures in UIDAI along with a dedicated security team to implement the various security processes and technology to ensure security of CIDR.

- UIDAI-CIDR is ISO 27001:2013 certified since 2015 and since then undergoes through yearly surveillance audits from STQC.

- GRCP-SP (Governance, Risk, Compliance, Performance service provider) has been appointed to perform periodic monitoring of the security of internal and external ecosystem.

- The security audit of UIDAI is conducted by three separate entity viz. Internal, External (GRCP) and STQC on a periodic basis.

- Periodic assessments are conducted for the ecosystem partners to ensure compliance on the Information Security policy.

There are multiple layers of security at physical level in UIDAI Data Centres and is being managed by armed CISF personnel round the clock. Strengthening of security of data is an ongoing process and all possible steps are being taken in this regard. Further, Chapter VI (Protection of Information) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ("The Aadhaar Act") and the Aadhaar (Data Security) Regulations, 2016 framed there under, have been specifically drafted keeping in account the various security requirements in respect of data collected by UIDAI.

(e): The Aadhaar Act, 2016 and subsequent regulations framed thereunder, have adequate safeguards. Sharing of information or seeding of Aadhaar information with the authorised agencies is governed as per the provisions of the Aadhaar Act 2016. Section 29 (1) of the Aadhaar Act 2016 read together with Regulation 3(1)of the Aadhaar (Sharing of information) Regulations, 2016 categorically states that no core biometric information, collected or created under the Aadhaar Act, shall be shared with anyone for any reason whatsoever; or used for any purpose other than generation of Aadhaar numbers and authentication under the Act. Also, Regulation 4(1) of the Aadhaar (Sharing of information) Regulations, 2016 provides that core biometric information collected or captured by a requesting entity from Aadhaar number holder at the time of authentication shall not be shared for any reason whatsoever.

Regulation 4(2) of the Aadhaar (Sharing of information) Regulations, 2016 provides that identity information available with a requesting entity shall not be used for any purpose other than that specified to the Aadhaar number holder at the time of submitting identity information for authentication and shall not be disclosed further without the prior consent of the Aadhaar number holder. Further, Regulation (5) of the Aadhaar (Sharing of information) Regulations, 2016 ensures the responsibility of any agency or entity other than requesting entity with respect to Aadhaar number and subsequent Regulation (7) states that any contravention of the abovementioned regulations shall constitute a violation of sub-section (2) of Section 29 of the Act.

Section 30 of the Aadhaar Act, 2016 applies the rigours of the IT Act, 2000 and the rules thereunder whereby 'Biometric information' is deemed to be 'sensitive personal information'. Additionally, Chapter VII of the Act lays down monetary penalties and imprisonment for unauthorized sharing of residents' identity information. Any violation to the provisions of the Aadhaar Act, 2016 is a criminal offence.

******