

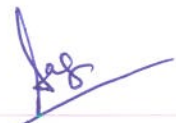
**Information Note to the Press (Press Release No. 78/2018)**

**Telecom Regulatory Authority of India**

**TRAI releases Recommendations on “Privacy, Security and Ownership of Data in the Telecom Sector”**

**New Delhi, 16<sup>th</sup> July, 2018:** The Telecom Regulatory Authority of India (TRAI) has today issued its Recommendations on “Privacy, Security and Ownership of Data in the Telecom Sector”.

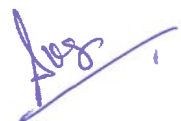
2. The Authority had suo-moto issued a Consultation Paper on “Privacy, Security and Ownership of Data in the Telecom Sector” on **9<sup>th</sup> August, 2017** with the following objectives:
  - (a) To identify the scope and definition of Personal data, Ownership and Control of data of users of telecom services..
  - (b) Understand and Identify the Rights and Responsibilities of Data Controllers.
  - (c) To assess the adequacy and efficiency of data protection measures currently in place in the telecom sector.
  - (d) Identify the key issues pertaining to data protection in relation to the delivery of digital services. This includes the provision of telecom and Internet services by telecom and Internet service providers (TSPs) as well the other devices, networks and applications that connect with users through the services offered by TSPs and collect and control user data in that process.
3. Comments and counter-comments received from the stakeholder were published on TRAI’s website. An Open House Discussion was also conducted in New Delhi on **01.02.2018**.
4. Comments and counter-comments received from the stakeholders along with the additional inputs received during the Open House



Discussion were considered by the Authority before formulating its recommendations.

5. The recommendations made by the Authority are as follows:

- (a) Each user owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem. The entities, controlling and processing such data, are mere custodians and do not have primary rights over this data.
- (b) A study should be undertaken to formulate the standards for anonymisation/ de-identification of personal data generated and collected in the digital eco-system.
- (c) All entities in the digital ecosystem, which control or process the data, should be restrained from using Meta-data to identify the individual users.
- (d) The existing framework for protection of the personal information/ data of telecom consumers is not sufficient. To protect telecom consumers against the misuse of their personal data by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem, which control or process their personal data should be brought under a data protection framework.
- (e) Till such time a general data protection law is notified by the Government, the existing Rules/ license conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem. For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers, and Applications.
- (f) Privacy by design principle coupled with data minimization should be made applicable to all the entities in the digital ecosystem viz, Service providers, Devices, Browsers, Operating Systems, Applications etc.



- (g) The Right to Choice, Notice, Consent, Data Portability, and Right to be forgotten should be conferred upon the telecommunication consumers.
- (h) In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.
- (i) For the benefit of telecommunication users, a framework, on the basis of the Electronic Consent Framework developed by MeitY and the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users.
- (j) The Right to Data Portability and Right to be Forgotten are restricted rights, and the same should be subjected to applicable restrictions due to prevalent laws in this regard.
- (k) Multilingual, easy to understand, unbiased, short templates of agreements/ terms and conditions be made mandatory for all the entities in the digital eco-system for the benefit of consumers.
- (l) Consumer awareness programs be undertaken to spread awareness about data protection and privacy issues so that the users can take well informed decisions about their personal data.
- (m) Data Controllers should be prohibited from using “pre-ticked boxes” to gain users consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.
- (n) Devices should disclose the terms and conditions of use in advance, before sale of the device.
- (o) It should be made mandatory for the devices to incorporate provisions so that user can delete pre-installed applications if




he/she so decides. Also, the user should be able to download the certified applications at his/ her own will and the devices should in no manner restrict such actions by the users.

- (p) Department of Telecommunication should re-examine the encryption standards, stipulated in the license conditions for the TSPs, to align them with the requirements of other sector regulators.
- (q) To ensure the privacy of users, National Policy for encryption of personal data, generated and collected in the digital eco-system, should be notified by the Government at the earliest.
- (r) For ensuring the security of the personal data and privacy of telecommunication consumers, personal data of telecommunication consumers should be encrypted during the motion as well as during the storage in the digital ecosystem. Decryption should be permitted on a need basis by authorized entities in accordance to consent of the consumer or as per requirement of the law.
- (s) All entities in the digital ecosystem including Telecom Service Providers should be encouraged to share the information relating to vulnerabilities, threats etc in the digital ecosystem/ networks to mitigate the losses and prevent recurrence of such events.
- (t) All entities in the digital ecosystem including Telecom Service Providers should transparently disclose the information about the privacy breaches on their websites along with the actions taken for mitigation, and preventing such breaches in future.
- (u) A common platform should be created for sharing of information relating to data security breach incidences by all entities in the digital ecosystem including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem including all such service providers to be a part of this platform.



(v) Data security breaches may take place in-spite of adoption of best practices/ necessary measures taken by the data controllers and processors. Sharing of information concerning to data security breaches should be encouraged and incentivized to prevent/ mitigate such occurrences in future.

6. The recommendations have been placed on TRAI's website [www.trai.gov.in](http://www.trai.gov.in).
7. For any clarification/information Sh. Sunil Kumar Singhal, Advisor (BB&PA) may be contacted on Tel. No. +91-11-23221509 or email: [sksinghal@trai.gov.in](mailto:sksinghal@trai.gov.in).

  
(S.K. Gupta)  
Secretary, TRAI