Tabular Mapping Of Stakeholders' Responses To Question 3 - TRAI Consultation Paper: Rights, Responsibilities And Regulation Of Data Controllers

---

The following table was prepared after an analysis of all fifty-three (53) responses to Question 3 of the Consultation Paper, *"What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers".* The table identifies the issues raised by the stakeholders and their stances in response to the question. It also states the suggestions they have made to the TRAI in view of the question posed. As mentioned earlier, the responses of the stakeholders have been categorised in a manner that corresponds with some of the issues raised in Part III and part IV of the White Paper, particularly the concerns related to the rights and responsibilities of the data controllers, prioritization of rights of the data subject, and effective accountability and enforcement tools.

Sl. No	Stakeholder	Issues Addressed			Comments/recommendations	
		Rights and Responsibilities of Data Controllers	Rights of the Data Subject	Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data?	Regulatory Approaches	Accountability and Enforcement Tools

1	Internet and Mobile Association of India (IAMAI)	Any personal data can have multiple Data Controllers (DCs) depending on the usage of such data by the users. 'Rights and Responsibilities' must be devised keeping the following distinctions between the stages of data handling in mind: I. Data in transit (data subject → DC, often handled by a third-party data processor), exposed to ISPs. II. Data after completion of transit (once it reaches the DC), over which users (through their devices) have control. Expressly set out rights of DCs in the proposed data protection law. Copyright laws should recognize the rights of DCs with regard to proprietary rights over datasets. Onus of proving due diligence must be on the organisation in case of breach/complaint.	__	No, unless for reasons of national security or public interest. Data subjects (DS) voluntarily offer their personal data for the convenience of customised services, and DCs profit from providing those services. It is symbiotic relationship.	Define"data controller" in a clear and precise manner.The Asia Pacific Economic Cooperation (APEC) Privacy Framework, drafted with the digital economy in mind, is business friendly and user centric, and should be considered when formulating the law. Define broad principles and requirements, allowing organizations to design their own privacy programs based on due diligence guidelines, instead of prescribing privacy practices in form of administrative requirements. Internet Service Providers (ISPs) may use information provided by users to various service providers, in order to use applications / websites, in a manner that	Encourage industry specific self-regulation, while holding them accountable for violations of the guideline. Supplement legislations with an adequate implementation ecosystem, with grievance redressal systems, user awareness, research, etc.

					is not consented to by the provider. For example, to aid advertising and promotion purposes without the express/informed consent of the DS. Therefore, in order to empower the user with regard to her/his data as well as retain the functionality of the service, a rights and consent based approach must be adopted.	
2	Association Of Competitive Telecom Operators (ACTO)	Limitations on usage of personal data should be qualified and proportional to the risk their misuse. Data should be collected and used only for a specific stated purpose. Only necessary amount of data for the stated purpose must be collected no more. Businesses should take proactive measures to implement concepts like privacy by design and data breach notification, consistent with the principle of accountability, and self regulate, demonstrating their	If personal data is to be re-used for a different purpose the DS should be informed and provided with a measure of control prior to such use.	__	Analyze the economics of remedies and sanctions by enforcement authorities. Enhance international regulatory cooperation and interoperability of regulatory frameworks. New technologies(Big Data, Internet of Things) do not necessitate new regulations. A balance of traditional standards and new methods, in light of their tremendous potential, flexible enough to allow	Establish a special regulator to supervise compliance with the statute more proactively and deal with contraventions of the legislation. Regulation must be through an office of Ombudsman.

		willingness and ability to take on data responsibility and ensure compliance on an ongoing basis. De-identification and pseudonymization should be encouraged.			for innovation and development of future consumer and societal benefits of collecting and using such data, suffices. Regulation must be light handed.	
3	The Associated Chambers of Commerce and Industry of India (ASSOCHAM)	IT Act and Rules clearly lay out rights (for users) and responsibilities (for controllers). Rights of controllers to also process user data in other legitimate manners to generate additional user value must be recognised.	__	No one set of rights should be seen as superseding or obtaining precedence over another. The rights of the DCs and individuals must be balanced. Users decide to part with their data in exchange for specific services or products and this element of volition and user choice must be respected.	__	
4	Cellular Operators Association of India (COAI)	__	Obtaining specific consent of the DS for use of information in an anonymized format	__	While Telecom Service Providers (TSPs) acting as DCs notify users of collection of data and the purpose for collection,	__

			should not be mandatory.		regulatory principles need to be formed for other digital entities to act as DCs. These principles should be made applicable to Telcos as well.	
5	Global System for Mobile Communications (GSMA)	__	__	No, and compliance must allow them to reassure public of the same.	Set out the principles which controllers are expected to uphold (Eg: National Level Privacy Principles proposed in the Report of the Group of Experts on Privacy).	Encourage adoption of comprehensive internal compliance programmes which demonstrate compliance to consumers and regulators. This allows DCs flexibility in terms of how business is conducted and supervision by regulators where it matters rather than being inundated with prior authorisation requests.
6	Internet Service Providers Association of India (ISPAI)	The rights and responsibilities of the DC during the usage of customer personal data should be similar to those of other entities in the Internet Ecosystem. DCs should adhere to all the laws/ guidelines/ compliance	Consolidated data of the DS must not be sold anonymously or otherwise.	No, as customer rights and personal data protection should be respected.	__	__

		requirements on privacy and personal data protection which they are subjected to.				
7	National Law University Delhi (NLUD)	The business and other activities of DCs should be regulated by data protection laws informed by sound data protection principles. Simple, clear and concise notice of information practices must be given before any information is collected. Individuals must be provided with a choice to opt in/out. Only such information as is necessary and adequate for the stated purpose must be collected. Notice and consent are a must before giving access to third parties. Reasonable security safeguards against loss, unauthorised access, use or destruction of Personal Information must be employed. All necessary steps to ensure compliance with the privacy principles must be taken.	Individuals must have access to the information collected from them and they should be able to seek corrections, amendments, or deletion where inaccurate. They must also have access to information regarding compliance with privacy principles. Data breach notifications must be provided in high risk cases.	In certain circumstances, DC must not permit the sharing of data, even if the DS is inclined to share it as it would be inconsistent with the reading of the right to privacy into the right to life, and with the principle that individuals cannot voluntarily alienate this right.	Adopt General Data Protection Regulation (GDPR) as the base on which any new regulations are built: The DC should be made accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies, including training and education, audits, etc. It must be made possible to object to processing of information on compelling legitimate grounds including direct marketing uses. Limit automated decision-making.	Self-regulation and co-regulation must be encouraged. Provide recourse to the courts to enforce data privacy rights and allow class action suits by public interest privacy groups. Establish an Independent Data Protection Authority (DPA) to make decisions and issue administrative sanctions, including fines. The DPA must have the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis. Mandatory appointment of data protection officers

					Data breach notifications to DPA and DS in high risk cases. Institute opt-in requirements for marketing.	in companies that process sensitive personal data.

8	Span Technologies	—	—	—	—	A dedicated, independent, autonomous DPA with a well-defined mandate for data and privacy protection needs to be set up at national level reporting only to the President of India. It should have a complete oversight for implementing the Privacy and Data Protection Law and interact with the government, industry and users to oversee observance of fully secure data integrity practices. It should also enjoy legislative backing to look into complaints, investigate breaches through comprehensive audit and layout corrective course of action with mechanisms for redressal that needs to be implemented.

						It should have judicial powers to prosecute and punish violators of privacy and data security norms as defined by the law.
9	TRA	__	__	__	__	__
10	The National Association of Software and Services Companies (NASSCOM) - Data Security Council of India (DSCI)	DC should be subject to various responsibilities in order to exercise the rights granted by the Constitution of India and fulfill the individuals' demands, if any, while practicing their rights. DCs must inform individuals of such activities/processes where they are obligated to disclose to law enforcement agencies or retain personal information for any amount of time even after the individual has asked for it to be deleted. Also, data must be processed only for the specified purpose.	__	__	The roles of DC and Data Processors must be adequately defined along with corresponding obligations and practices. The APEC Privacy Framework may be referred to for the same. The legal framework should recognize self certification by DCs against misuse, unauthorized sharing, etc. to instill confidence in users. Make sector specific regulations complementing data protection laws.	Establish DPAs at the national level and data protection officers and officers at the organisational level for enforcement and governance.

11	Association for Competitive Technology (ACT)	__	__	__	__	__
12	Zeotap India Pvt. Ltd.	DCs must be made responsible for transparency (notice), data security, secure processing of data and any data breaches due to processes adopted or otherwise.	__	No. Rights, including the right to privacy, of any individual are always prime, inline with the recent Supreme Court (SC) judgement.	Submission of audit reports to concerned authorities must be mandated for obtaining licenses or designating the entity as a body responsible for data protection and cyber security for the telecom sector/country.	Processes and personal data security systems must be regularly subject to third party audits.
13	Takshashila Institution	Process data such that no harm is caused to the DS. DC must be protected under the law if it proves that due diligence was exercised in processing data. DC must be held accountable for all the harm resulting from violations of data rights and must not be allowed to rely on consent obtained to limit its liability. DC must ensure that each individual must have the power to determine how much data he is willing to share with a DC.	DS cannot sue the DC over sharing of anonymised data if the data is not capable of being attributed to a specific person. The DS should have the power to decide how much data the DC can collect, process, disclose, or transfer.	__	Department of Telecommunications, Telecom Regulatory Authority of India (TRAI) and other security agencies of the government that have access to personal data or issue telecommunications licenses should be included in the definition of DCs. In case of harm to a DS, investigation should be carried out by "*learned*	A Data Commissioner must be appointed whose must set appropriate standards for DCs to adhere to and update the same in a timely fashion to stay relevant with technological advancements. He must also have the power to investigate cases of improper processing and pass appropriate orders.

		The DC must ensure the security of the data collected and will be liable for any security breach, even in the absence of any harm.			*intermediaries*", i.e., entities capable of evaluating the output of algorithms used by DCs, identifying instances of data rights violations detecting biases and suggesting remedial measures. They may be persons drawn from the private sector proficient in personal data processing and data driven decision making.	
14	Information Systems Audit and Control Association (ISACA)	Data must be used only for the purpose and duration that it was collected for. The DC must adhere to and have expert knowledge of all applicable data protection laws, regulations and practices affecting them. Issues like information and data security are enterprise-level concerns, DCs must report directly. TSPs must provide opportunities for individuals to report issues, akin to the current ombudsman structure in place for reporting complaints.	Individuals must be provided with opportunities to repost issues.	No, unless for reasons of national emergency or security. Rights, including the right to privacy, of any individual are always prime, inline with the recent SC judgement.	—	Create a Data Control Authority to govern, regulate and educate DCs and centralize the same to enable streamlined two-way communications, enabling better information dissemination to all involved.

15	International Business Machines Corporation (IBM)	__	__	__	A framework of accountability fixing must be set up instead of deploying DCs as creation of a capable auditor workforce would be difficult and the industry will not welcome auditing of proprietary information. Under this framework, all entities must adopt sufficient security measures(encryption, anti-hacking, antivirus, avoid back door access by data supply chain entities, etc.) and be made responsible for personal data collection, processing and/or use, irrespective of legalities involved.	__
16	Make My Trip	Should obtain consent of individuals, which mentions the purpose and nature of third party, before sharing information with them.	Users must have the option to retract or limit their consent.	__	Define "Data Controller" and "Data Processor" in general parlance. DC should not be made liable for breach for sharing information as a part of a specific	__

		Share user data only with parties who have adequate security mechanisms to protect the data.			transaction made by users. (Eg: sharing of passenger information with airline by online travel agency). Also, DC should not be made liable for breach by the third party in such specific transactions. The respective third party must be held liable. Such third parties should not be considered data processors as they merely use the data for the limited purpose of the transaction.	
17	Access Now	Obligations: consent, storage duration, purpose, adequate security measures, bar against unauthorized disclosure. Where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved. DCs should not use or share data, with anyone including with affiliates,as it is a clear violation of the right to privacy.	DS must have access to the data and must be able to correct if necessary.	__	__	__

		Data breach notification that is timely, easy to understand and comprehensive should be given to the authorities, and, remediation options should be clearly indicated and accessible. It should not contain any personal information which should only be shared pursuant to a proper legal process and request.				
18	U.S. India Strategic Partnership Forum (USISPF)	They should give users notice of privacy practices; to seek informed consent; not collect more personal data than is required; to seek consent before disclosing personal data; to make personal data available to the users; to handle data securely and to handle sensitive personal data with additional protections. Onus of proving due diligence must be on the organisation in case of breach/complaint. DC must meet privacy obligations and provide redress to individuals. Data processor must follow and assist the DC in doing the same. They will be liable for any demonstrable fault of theirs.	__	Question of supersession does not arise as there is no dichotomy between rights of DCs and individuals.	The APEC Privacy Framework, drafted with the digital economy in mind, is business friendly and user centric, and should be considered when formulating the law. Define broad principles and requirements, allowing organizations to design their own privacy programs based on due diligence guidelines, instead of prescribing privacy practices in form of administrative requirements. Maintain the current distinction in responsibility	__

					between a DC, which determines the means and purposes of processing data and a data processor, which processes the data on behalf of another organization. There should be no interference in the contract governed 'controller-processor' relationships.	
19	Information Technology Industry Council (ITI)	Adopt adequate security measures. Take reasonable steps to deal with privacy inquiries or complaints.	__	__	Rights of DCs and DSs should not be at odds. Adopt an accountability-based system that clearly defines and apportions liability between DCs and data processors. Adopt forward-looking privacy and data protection models which focus on DCs ensuring that their processing operations do not violate individuals'	__

					rights or overburden individuals. Require organizations to incorporate "privacy by design" into their products.	
20	Sigfox	Specification of purpose. Security measures must be adopted, including anonymization where necessary.	__	No	A balanced multi-stakeholder framework that allows the development of the IoT ecosystem while ensuring individual's rights to protect and control his/her Personal Data should involve designers, manufacturers, network operators, service and application providers, regulators and end users. Privacy and data laws should enable inclusive approaches.	Create collaborative bodies in-order to involve all stakeholders which oversee the development of ethical practices while ensuring users are able to negotiate on an equal footing with data collectors.

21	Exotel Techcom Pvt. Ltd.	DC should have the right to collect only when: 1. DS has provided informed consent following adequate notice 2. Data processing is needed for a contract.(Eg: billing, job application, loan request, etc). 3. Group, not individual level of processing the data will improve service offered to DS. 4. Transfer of data is solely to enable fulfillment of service. 5. Processing is required as per applicable law. DC must be under an obligation to: 1. Collect, process, use and/or transfer data only when legal, fair and for explicit and legitimate purposes. 2. Easily accessible and visible provisions to rectify/remove incorrect personal information within 7 days 3. State expiry period for stored personal information,	DS must be able to modify preferences, completely prohibit the use of their personal data (except under any applicable law) and specify additional purposes for which it may be used through a call, message, platform, etc. Customers/DS must be notified of all breaches, including those suspected/anticipated.	No, legal ownership and control of personal data must always remain with the relevant individual.	The scope of personal data should be clearly defined and must include: 1. Financial information 2. Caste, religion, sexual orientation 3. Medical records and history 4. Biometric information 5. Web browsing history across devices 6. App usage history 7. Content of the person's communication 8. Geolocation 9. Social security numbers - Aadhaar , voter id, passport etc 10. Derivatives which can include personal preference and habits inferred or identified from personal data.DC must be registered, subject to meeting the prescribed data protection and security standards, in order to collect, use, process or share data and must be classified based upon the	Establish a DPA to provide a platform for registration, monitor compliance, investigate breaches and complaint, and, direct the DC to do/omit to do something, impose monetary penalty based on the sensitivity of data and suspend/shutdown services of DCs based on gravity of violation.

		not retain the same for longer than necessary and discourage hoarding of data. 4. Protect against alteration or unlawful disclosure with appropriate security measures. 5. Establish 2-tier grievance redressal system with QoS to respond to and resolve complaints regarding data breaches within 5 days and escalate to the DPA if DS has not receive an adequate answer within 15 days. 6. Notify the DPA of the purpose and/or proposal for collection of data for use/processing.			nature and scope of their business. Standard certification for data security requirements should be incentivized. The purpose must be directly related to the service/product being offered Notice in a standardized format, prescribed by the DPA, with list of data points to be collected, purpose, third parties with whom it may be shared, applicable law and duration of storage, must be issued, which avoids complicated language, mentions the DCs involved and lets the DS specify the duration, limit the purpose of consent and set the expiry date for storage.	
22	KOAN	The rights and responsibilities of DCs and data processors should be determined by the contractual	Rights of individuals, such as choice and access, should be respected.	__	__	__

		arrangements between them, as well as between the DS and DC. Should be defined by principles of accountability, minimisation, purpose and collection limitation, as also identified by the AP Shah Committee.				
23	Internet Freedom Foundation (IFF)	All TSPs should publish privacy policies, report any data breaches to affected users, TRAI and the Dept. of Telecom.	Users should be given notice of any data breach.	No. data protection is about protecting the user, not the data.	Focus on TSPs. Examine existing privacy and data protection provisions as applicable to TSPs which need greater enforcement and improvement.	Have penalty provisions to enforce obligations.
24	Mozilla Corporation	Meaningful notice, choice, and consent mechanisms must be offered. Limit collection and purpose. Facilitate access, correction, and the right to object. Provide security and role based access control and protections against unlawful disclosure. Train employees and contractors. DC must at all times be able to demonstrate to the DPA that any data processing has been done in	__	No. Right to privacy of any individual is of paramount importance, inline with the recent SC judgement.	__	Empowered and independent data protection authority should be created for the purposes of regulation, training, oversight, and enforcement pursuant to the data protection framework.

		compliance with the data protection framework. Adopt appropriate technical and organizational measures and publishing policies. Ensure adequate documentation of all data processing decisions and actions.				
25	Internet Democracy Project	Comply with, plan and implement policies in line with principles of data protection. Obtain consent of DS and be in a position to demonstrate the same. Refer to responsibilities of DC mentioned in the GDPR.	DS cannot sue the DC over sharing of anonymised data.	No, except for when data has been sufficiently anonymized and when DC has to cooperate with law enforcement agencies for narrow and specific requests. The processing in such cases should be proportionate to the aim being pursued.	Refer to EU Data Protection Directive and GDPR for definitions/concept of DC and data processor. Merely assigning responsibilities to DCs is insufficient. Introduce responsibilities and sanctions for 'data processors' as well. Since many processing functions are outsourced to third parties, they should be envisioned within the framework, as well.	An independent national supervisory authority must oversee the functioning of DCs.

26	Citibank	DCs must have a right to protect their business and operations against misuse of rights by consumers in providing consents. DCs must maintain secrecy and not divulge information, prevent unauthorized interception of messages, practice openness in implementation of practices/procedures/policies, be accountable for harm resulting from violations, have limitations on collection and purpose of processing, give upfront notices to the consumers etc.	__	No. Rights of the DCs are subject to the rights of the individuals who provide the capital, i.e. personal data.	Misuse of rights by consumers should incur punitive action.	Subject DCs to regulatory audits through regulators like TRAI or any delegated authority.

27	Indian Software Product Industry Round Table (iSPIRT)	*Rights*: DCs may co-create data with users and retain a copy of such generated data. DCs may demand for data that is proportional to the feature they are enabling. *Responsibilities:* Safe and secure storage of data. They will be liable for unauthorized access/sharing. Notification of purpose of collection. Collection of only proportionate amount of data. There must be no personal data record-keeping systems whose very existence is secret to the subscriber. Publish regular, easy to understand statements about their practices for users.	Anonymised data sets may be shared without user consent. Users must be allowed complete access to their data in a human-readable and machine-readable format. They should be able to seek corrections and amendments where data is inaccurate. Users should be allowed to share their data with other service providers in a safe and secure manner. Users must be notified in case of a data breach.	__	TRAI should allow / facilitate the sharing of anonymised / aggregated data to enable innovation in this space. Periodic Privacy Impact Assessments and Security Impact Assessments must be conducted.	TRAI should monitor the statements by DCs for abusive practices, proportionality, etc. Complaints about disregarding practices should be managed by TRAI through a customer grievance cell.
28	The Centre for Internet and Society (CIS)	Powers of DCs should be strictly limited by the consent provided by DSs and/or as required by law.	If personal data is to be re-used for a different purpose the	If the DC can demonstrate existence of legitimate interest, it	__	__

		Data should be collected and used only for a specific stated purpose.	DS should be informed and provided with a measure of control prior to such use.	may be allowed to process data for purposes other than those expressly consented to. Factors for determining legitimate interest include reasonable expectations of DS, adverse impact of processing on DS, overriding public interest, sensitivity of data, relationship and power positions of DC and DS, and measures taken by the DC to reduce impact on the privacy of the individuals.		
29	US India Business Council (USIBC)	DC must meet privacy obligations and provide redress to individuals. Data processor must follow and assist the DC in doing the same. They will be liable for any demonstrable fault of theirs.	—	—	Maintain the current distinction in responsibility between a DC, which determines the means and purposes of processing data and a data processor, which processes the data	—

					on behalf of another organization. Future legislation should recognise that DCs have proprietary rights over anonymized, purposely-designed datasets.	
30	Disney Broadcasting (India) Ltd	__	__	__	__	__
31	Business Software Alliance (BSA)	There must be a clear allocation of responsibility and liability to ensure that the increasingly widespread practice of outsourcing does not create uncertainty. DC must meet privacy obligations and provide redress to individuals. Data processor must follow and assist the DC in doing the same. Direct, joint, or several liabilities or other obligations should not be imposed on data processors.	__	__	Accountability based framework should be adopted.	__
32	IT for Change (ITfC)	DCs should act as trustees of user data and services developed must be in strict trusteeship for users. It	__	DCs rights are within and subservient to individual rights.	Law and regulation must be based on the principles of data ownership and value. As the matter	__

		must be ensured that value creation does not harm the trusteeship.			concerns civil, social and commercial rights, it may be put into the constitution, or read into it. Database businesses with a large number of users must be subject to close regulatory scrutiny, such that it does not hamper the growth of the digital economy.	
33	Software Freedom Law Centre (slfc)	*Rights:* 1. To collect and process the necessary amount of information to provide specified service for a limited period of time. 2. To use higher standards of security than specified. 3. To innovate through improvement of the security of their products and services. 4. To not be forced to weaken security or build backdoors. *Responsibilities:* 1. To collect and process only for the specified purpose	DS must be notified of data breaches that affect them. DS must be notified of purpose, data collected, grievance redressal mechanisms, effect of agreeing/disagreeing, third parties, etc. Such notice must be simple, easy to understand and available in English and one vernacular language.	Only in certain specific circumstances: 1. Necessary for compliance with law. 2. Part of the public domain. 3. Necessary to provide service.	There should be an oversight mechanism for Rule 8 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 to ensure that DCs are taking enough measures to protect the data.	Since CERT-In already deals with security of data, the powers of CERT-In to regulate and decide upon issues of data security could be expanded, and a new body(DPA) could be established to deal with issues of data privacy- to monitor compliance, investigate breaches and complaint, and, issue directions and orders.

		2. To ensure the security of personal and sensitive personal data. 3. To give notice of data breaches to Computer Emergency Response Team of India (CERT-in), sectoral regulators and affected DSs. 4. To share user data only with parties who have adequate/ same standards of security and privacy, after obtaining consent of DS. 5. To transfer only to countries with reciprocal levels of protection. 6. To not publish personal data 7. To be open about procedures and practices adn to publish the same. 8. To train their staff in security procedures. 9. To restrict access to data to only to whom it is necessary to perform their duties.				
34	EBG Federation (EBG)	Responsibilities: give notice, seek informed consent, minimize collection, do not repurpose	DS cannot sue the DC over sharing anonymized data sets.	No conflict between DC and DS rights recognised in SPDI,	DCs rights over anonymised, purposively-designed	DC and data processor must be distinguished/defined

		collected data, delete after expiry, obtain consent before sharing with third party, make data available to relevant users, handle data securely and handle sensitive data with special care. When an organisation is required by law to process personal data, it cannot negate its responsibility by 'handing over' responsibility for the processing to another DC or data processor.	DS should have access to their data. DS must be notified and their consent must be obtained before data is shared with third parties.	their relationship is voluntary and symbiotic.	datasets should be recognised.	clearly to determine liability in case of data breaches.
35	AT&T Global Network Services India Pvt. Ltd. (AT&T)	Onus of proving due diligence must be on the organisation in case of breach/complaint.	—	DC and DS are not necessarily in conflict.	Clearly define DC. Users must be empowered without over regulating the DC. Policy should focus on preventing harm and misuse and improving accountability. Follow well-established international standards Eg: APEC framework which is drafted with the digital economy in mind, is business friendly and user centric.	Encourage industry specific self-regulation, while holding them accountable for violations of the guideline.

					Define broad principles and requirements, allowing organizations to design their own privacy programs based on due diligence guidelines, instead of prescribing privacy practices in form of administrative requirements. Focus must be on building the necessary ecosystem and not just on DCs, in light of the comprehensive data privacy law being designed by the government which will be applicable across sectors.	
36	Broadband India Forum (BIF)	Responsibilities: give notice, seek informed consent, minimize collection, do not repurpose collected data, delete after expiry, obtain consent before sharing with third party, make data available to relevant users, handle data securely and handle sensitive data with special care.	Data collected from DSs should not be repurposed without their consent.	Rights of DC and DS are not in conflict, their relationship is voluntary and symbiotic.	DC must be clearly defined to apportion responsibility. To not hamper innovation users must be empowered without over regulating the DC. Policy should focus on preventing harm and	—

		DC must meet privacy obligations and provide redress to individuals. Data processor must follow and assist the DC in doing the same.			misuse and improving accountability. TRAI should support privacy guidelines developed by industry and other stakeholders before moving toward regulation. Eg: industry voluntary efforts, best practice codes and multi-stakeholder initiatives. Regulations must be light-touch, flexible, based on general standards and not overly prescriptive. Distinguish between data processors and DCs.	
37	Sangeet Sindan	Obtain explicit consent. Processing must be fair and legitimate. Appoint a data officer ensuring compliances and dealing with complaints by DS. Conduct periodic audits of outsourcing company.Mention data retention policy in user agreement along with the period of retention. Include standard minimum terms in data sharing agreement. Take appropriate technical and	Individuals must have access to the information collected from them and they should be able to seek corrections, amendments, or deletion where inaccurate.	__	DC must be defined in law.	__

		organisational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.				
38	Redmorph	__	__	__	__	__
39	Baijayant Jay Panda	Collection and processing must be fair, lawful and transparent. DC must maintain confidentiality and take adequate security measures. Maintain accurate records of data collected, accessed, stored and processed.	In case of data breach affected DS must be notified within 7 days.	No.	Establish a quasi-judicial body to regulate, govern, undertake *suo moto* inspection and monitor compliance of DC.	__
40	Apurv Jain	__	__	__	__	__

41	Reliance Jio Infocomm Limited (RJIL)	The rights and responsibilities of a DC as distinct from those of telecom subscribers may be derived from the Unified License. Implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the regulation. Implement appropriate data protection policies and demonstrate compliance whenever asked for by the regulator.	Disclosure of personal data must only be with the explicit consent of the DS, barring designated LEAs, anonymized datasets and cases involving national security, public interest, etc, as already mentioned in the Licensing Terms and Conditions. DS should be able to access his/ her data at any point of time or require the DC to return and destroy such data.	No, except for reasons of national security.	Define DCs as different agencies through their operational functions collect, store and process data in different forms and formats. Refer to the EU GDPR for definitions of controller, processor, recipient and third party, and use them interchangeably for an organisation having all four capabilities. Guidelines for data protection should provide for supervisory authorities and certification bodies.	The relevant authority must be able to enforce the requirement to share access and control over data and must have the ability to track the data flow.
42	Bharti Airtel Limited	Responsibilities and rights of DCs should be similar to the entities dealing with the processing and collecting of the customers' data.	Resale of data must be restricted irrespective of whether it's consolidated,	No.	Set out the principles which DCs are expected to uphold.	__

			anonymous or otherwise.		Encourage adoption of comprehensive internal security programs. Restrict on-selling of consolidated data, anonymous or otherwise.	
43	Idea Cellular Ltd.	Notice must be given before taking individual consent in simple, clear and concise language, regarding practices followed, including disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc, Declarations in respect of such information can be a part of the Organizations' Privacy Policy. Collect personal information from DS only as is necessary for the purposes identified and they should be able to seek corrections and amendments where data is inaccurate. Use reasonable security safeguards against loss, unauthorized access or use and destruction.	Individuals must be provided with a choice to opt in/out with regard to providing personal information. Consent is not necessary in case of anonymized/aggregated data or if the information is not personal in nature. DS must be notified of any data breaches.	No, except for reasons of public emergency, public interest, national security, maintaining friendly relations with foreign state and/or maintaining law and order.	Genuine privacy concerns exist in the case of players other than TSPs in the digital ecosystem who are only subjected to a limited mandate. Strong privacy and security laws that are equally and uniformly must be used to regulate entities in the ecosystem that deal with personal or sensitive data. Regular audits must be conducted by third parties to assess compliance and certify the DCs. Make privacy certification on compliance with "*Data Privacy Principles*" a requirement.	—

		Take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity of the data collected. Ensure compliance with the privacy principles. The information regarding the same must be made in an intelligible form, using clear and plain language, available to all individuals.				
44	Mahanagar Telephone Nigam Limited (MTNL)	Rights of DC should be limited to offering services and products only. *Responsibilities:* Obtain, use and disclose data fairly for specified, explicit, lawful purpose. Ensure data is adequate, relevant and not excessive. Keep data safe, secure, accurate, complete, up-to-date and only till expiry of consent.	DS must be provided with a copy of the data on request.	No.	Implement an audit and certification system.	__
45	Reliance Communications Ltd.	The DCs should have obligations, similar to TSPs, to protect users personal data. DC must obtain prior consent, specify purpose and ensure security of collected data.	Consent of the DS needn't be obtained by the DC to share anonymized datasets.	No, except for reasons of national interest.	DCs must be made to register themselves through an online process with TRAI. For effective regulation and governance, local hosting of apps and their	TRAI should impose suitable penalties, similar to TSPs, for any breach of privacy of the user. TRAI should be empowered to order

		Data may be shared by the DC for commercial purposes where the user has consented to the same or when anonymized in certain cases.			databases should be mandatory.	blocking of content violating these norms.
46	Tata Teleservices Ltd. (TTL)	Give notice to user in a transparent manner containing data points collected, purpose, use, consent of user to share with third parties, security and safeguards established and contact details of privacy officer for filing a complaint. Collection and processing must only be for the specified purpose. Comply with measures to give effect to privacy policies, such as training, education, auditing, etc.	DS must be provided with the information regarding the process to access and correct personal information.	No.	—	Implement a co-regulatory enforcement regime as recommended in the Planning Commission Report, Oct 2012: ● Establish an office of Privacy Commissioner at both regional and central levels who will be the primary authority for enforcement of provisions. ● Emphasise self-regulation subject to regular oversight by the Privacy Commissioner. ● The courts will still be available

						as a forum of last resort in case of persistent and unresolved violations.
47	Bharat Sanchar Nigam Limited (BSNL)	Obtain and use data only with explicit consent and for specified purposes. Keep data safe, secure and protect against accidental loss or destruction of, or damage to, personal data. Notify TRAI of all processing of personal data and of any changes to processing, purpose, DSs, classes of data held, recipients and overseas transfers. Deep packet analysis must not be practiced. Ensure data is adequate, relevant and not excessive. Have standards for maintenance of records for processing of data, method of notification in case of data breach and standard operating procedures for the same. Have complaint mechanisms in place.	__	No.	__	__

48	Telenor	DCs rights over sensitive personal data obtained from users residing in India would depend on the form of data i.e. raw data or processed data. Implement appropriate technical and organizational measures to ensure and demonstrate that processing is performed in accordance with GDPR. Implement data protection policies and ensure data protection by design and by default. Process only as much as as specified. In case of joint DCs, determine respective responsibilities in a transparent manner and inform contact point for DS. Only use processors providing sufficient guarantees to implement measures as per GDPR requirements. Process personal data under the authority of the controller or processor. Cooperate with supervisory authority.	Individuals must be able to seek corrections, additions, amendments, or deletion. DS must be notified of data breaches.	DCs right may take precedence in certain specified circumstances as addressed by the GDPR.	Align subsequent regulations with GDPR to provide a consistent global approach that will enable business while protecting consumers. Awareness and transparency should be the pillars of maintaining privacy of personal data in the initial phase of privacy legislation.	__

		Ensures security of the personal data. Notify supervisory authority and DS of personal data breach. Carry out data protection impact assessment and identify the risk involved in processing under the advice of data protection officer. Consult with supervisory authority prior to processing high risk personal data in the absence of risk mitigation measures taken by the controller.				
49	Vodafone	Ensure confidentiality of personal communications. Respect permissions and preferences. Protect and secure information.	DC may generally use data collected form DS in an anonymized format for data analytics for innovative products and services.	No except for reasons of security, etc.	Advancements in technology must be accounted for. No restriction should be placed on the use of metadata as it does not in any way identify the individual consumer, but uses the trends, behaviours, etc for market analytics, innovative services, creation of new businesses, etc	—

50	Federation Of Consumer And Service Organization	__	__	__	__	__
51	Consumer Unity & Trust Society(CUTS)	DCs should make such disclosure in a simple and standard format, with multi-lingual accessibility, allowing consumers to report any misrepresentation or violation grievances and hold the DC accountable. DC may use personal information with informed consent of DS and DS must be allowed access to the data to ensure their right to portability. DC should be held responsible for data breaches by data processor.	Consumers must be empowered through a defined information disclosure mechanism to understand how and for what their data is being used.	No, unless for reasons of national emergency or security. This would help in plugging out anti-social elements, while providing rightful access to responsible consumers.	Private and government DCs should be treated alike to put the data protection regime in place. A suitable tech-framework coupled with futuristic and non-restrictive regulatory framework which promotes competition, and at the same time, does not pose hurdles for future innovation. should regulate and govern DCs.	__
52	Consumer Guidance Society	Interests of DCs and individuals should be balanced in determining rights and responsibilities. Data must be used only for the purpose for which it was procured. Obtain explicit consent of DS before sharing with third party as individuals are the owners of personal data.	__	__	__	__

53	Consumer Protection Association	Personal information should be adequate, relevant, not excessive, accurate, up-to-date, fairly and lawfully processed in line with DS rights, not stored beyond authorization, secured and not transferred to other countries without consent and adequate protection. Register with TRAI prior to processing any data. Notify TRAI of possible data breaches. Appoint data protection supervisors. Take appropriate technical and organisational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Create and make available the description of data file. Consult with the supervisory authority before processing specific types and categories of data. Document all processing systems used and provide information to the supervisory authority so that it can perform its duties.	__	No.	TRAI should: ● Monitor the development of information and communication technologies and their impact the protection of personal data ● Consult with CAGs, institutions and bodies on legislative and administrative measures relating to the protection of individual's rights and freedoms ● Be consulted on processing operations. ● Promote awareness of privacy standards, etc ● Advise DSs in exercising the rights laid down in provisions.	TRAI should: ● Monitor and ensure application of directive. ● Hear and investigate complaints. ● Serve legal notices compelling DCs to implement provisions. ● Check the lawfulness of data processing. ● Authorize officers to enter premises to investigate. ● Assist other supervisory authorities to ensure consistent application of provisions. ● An individual should be entitled to compensation from DC for damages caused from non-compliance.

					• Publish an annual report which names, in certain cases, those DCs that were the subject of investigation or action. • Prepare a code of practice for the sharing of personal data. • Assist in cases involving processing for special purposes.	• Failure to comply with an enforcement notice, information notice, or special information notice should be a criminal offence.