Brief on the Justice Srikrishna Committee White Paper On Data Protection Engagement and Process

Background

The Government of India through the Ministry of Electronics and Information Technology has formed the Justice Srikrishna Committee of Experts (link to composition of the committee) to suggest a framework for data protection in India (concerns on composition). The expected outputs of this committee is a data protection bill that would then be taken to Parliament to be enacted into a lage (link). The committee has released a white paper that runs into 233 pages and poses 231 questions (full pdf copy) inviting public comment. This document provides a short six page summary on the various issues listed in the paper given it's length and scope, to encourage wide public & expert engagement.

Public Comment: Timelines and Method

In response to the white paper, public comments have been invited from members of the public by *December* 31, 2017 (MyGov.in participation link). The form of public engagement (link) invites individual responses for each specific question or a general comment (link). At present paper based submissions can also be made by post in a prescribed format (link).

Components of the White Paper

The white paper is divided into five parts which have individual chapters. Within each part, the white paper sets out numerous chapters dealing with separate issues. Each of these chapters broadly follows a similar structure: *first*, the issue is set out; *secondly*, there is an account of comparative practice from other nations (primarily the EU, Europe, Canada, Australia, and South Africa); *thirdly*, the Committee's tentative view is set out; and *fourthly*, there are a series of specific questions for you to respond to.

Emphasis for commentators should be on a review of the provisional views and answering specific questions. If this is found difficult, commentators are urged to submit general comments (link). The *five component chapters of the white paper* are given in a tabular form after which each substantive chapter is individually explained and the key issues under them are set out.

Part 1	Context setting (Pages 1-23)	Gives a historical background of the paper including some broad approaches to data protection and informational privacy. These include foreign legislations, judicial precedent and existing and proposed legislative efforts.
Part 2	Scope and Exemptions	This is the first substantive chapter of the white paper that deals with specific issues such as the applicability of a data

	(Pages 24-75)	protection law to a geographic area (national and international), types of people (natural and artificial such as companies), the definition of personal data itself and to *whom* such a law (data controllers) should apply (for instance, should it apply for research or personal use). (myGov link)
Part 3	Grounds of processing, obligation on entities and individual rights (Pages 78-141)	These includes basic data protection principles on processing of data which requires notice to a person about their data and obtaining their consent. It also contains comments on the limitations on processing (limited to a specific purpose for user) and exceptions to this rule (public interest). It also contains storage limitations and comments on data quality, and the right to be forgotten. (myGov link)
Part 4	Regulation and Enforcement (Pages 143-203)	How (for eg. co-regulatory models that require codes of practice) and by whom the data protection framework will apply. It also invites comments on penalties on the nature of compensation and criminal offences. (myGov link)
Part 5	Summary (Page 204)	Seven key principles are identified which are incredibly important and form the backbone of the present consultation. (pdf link)
	Questions (Pages 205-233)	Chapterwise questions a total of 231 individual questions are listed. (pdf link)

Part II: Scope and Exemptions

Part II is titled "Scope and Exemptions". It lays out what areas a data protection law will cover, how it will cover them, and what will be exempt. It also addresses the possible interaction between a data protection law and existing laws that deal with data, such as the Aadhaar Act. A summary of the ten chapters in Part II with key concepts which are outlined in a table below.

1. Territorial and personal scope (Pages 24-29)	Any law passed by parliament defines the area to which it applies. This may be based on location, but in issues of data protection if the company which holds the data is not based in India but still offers services to Indians then data protection protections may be necessary. (MyGov link)
2. Other issues of scope (Pages 30-33)	The applicability of a law may be to a natural person (a human) or to artificial persons (such as a company/government). This part asks whether the rights to data protection can be available to either, or both. Further issues of scope such as should the law apply only to future conduct (data gathered subsequently) or retrospectively (data already held). (MyGov link)

3. Definition of personal data (Pages 34-40)	The applicability of the data protection law hinges on what is defined as, "personal data". This part focuses on what information, and its identification is capable of protection. It also has background on anonymous or pseudonymous data. (MyGov Link)
4. Sensitive personal data (Pages 41-43)	Many data protection legislations recognise two categories of data which is protected. While, "personal data" has some general protections, there is a higher level of protection which is given to, "sensitive personal data". Hence, sensitive personal data may include financial, health and caste information. (MyGov Link)
5. Definition of processing (Pages 44-47)	Processing consists of a bundle of activities (collection, use, analysis etc.) that are covered by Data Protection. Also if there are any differences between manual & automated processing. (MyGov Link)
6. Definition of Data Controller and Processor (Pages 48-51)	Any data protection requires that responsibility should be fixed on entities that hold and process data. This ensures accountability in the enforcement for which the data controller can include those who hold data (primary) or even who draw from such data banks (secondary). (MyGov Link)
7. Exemptions for household, journalistic & literary purposes & research (Pages 52-61)	In deciding the scope of data protection some activities and entities may receive a specific carve out. For instance, this would include people using their own data (CCTVs within homes), those used by private parties that serve a public purpose (journalists, artists, researchers) and state uses (lawful surveillance for preventing crimes). Several detailed questions are posed on the scope and specifics of such exemptions (MyGov Link).
8. Cross-border flow of data (Pages 62-68)	Given that data resides in multiple servers and data exchanges occur over multiple countries the governance of a national data protection law becomes difficult to administer without breaking these flows of data. To ensure the continuing benefit of data flows principles of adequacy of data protection laws within a foreign country that provide a comparable level of protection offer a solution (MyGov Link).
9. Data Localisation (Pages 69-75)	There have been growing demands for data of citizens to be locally stored, physically on servers located within a country. Such data localisation while may be appropriate for certain sensitive forms of data such as financial records but may fragment the global inter-activity benefits for other less sensitive forms of data (MyGov Link).
10. Allied Laws (Pages 76-77)	Quite often a single action is governed by several laws. Hence, which a comprehensive data protection statute will interact with several existing laws such as the Aadhaar Act. This chapter lists 21 statutes that may require amendment or reconciliation in various forms. (MyGov Link)

Part III: Grounds of Processing, obligations on entities and individual rights

Part III is titled "Grounds of Processing, Obligations on Entities and Individual Rights." This Part addresses the circumstances under, and the manner in which, your data can be "processed" by the State, or by other agencies. It also deals with the rights that you have over your data (before and after it has been processed), and the corresponding obligations upon entities that are holding and processing your data. A summary of the ten chapters in Part III with key concepts which are outlined in a table below.

1. Consent (Pages 78-84)	Any collection, analysis or storage of a person's data requires their consent. But often this legal principle even when put into practice requires greater effectiveness by which people can manage their digital services as per their will. (MyGov Link)
2. Child's consent (Pages 85-91)	India has a large population of children below the ages of 18 who being born digital use technology and part with data from an early age. Given that they may not be competent to understand the risks of parting with their data additional protections may be necessary. (MyGov Link)
3. Notice (Pages 92-98)	Before agreeing and to signifying consent a person should first be made aware of how they are parting with their data and how it will be used. Given the complexity of the existing framework of cumbersome terms and conditions urgent solutions are necessary so people know them rather than merely clicking on, "I Agree". (MyGov Link)
4. Other grounds of processing (Pages 99-104)	As an exception to the, "consent principle" some activities, as the paper notes, "it may not be possible to seek consent of an individual, prior to collection and use in all circumstances". However circumstances for such expectations (such as mandatory Aadhaar) are not indicated within the whitepaper. (MyGov Link)
5. Purpose specification and use limitation (Pages 105-110)	Any data which is gathered, stored or analysed is done pursuant to a purpose to which it is limited. Hence, data which is gathered for doing "A" cannot be used for "B". If there is a change in purpose then a person should have a clear notice, and option of consent for use of their data for "B". This way people retain control over their data. (MyGov Link)
6. Processing of sensitive personal data (Pages 111-116)	Sensitive personal data such as information such as a person's sexual activity or medical history may open them to a higher degree of harm (such as by social prejudice), and hence may require a higher degree of protection (bar from disclosure without consent). (MyGov Link)
7. Storage limitation and data quality (Pages 117-121)	As a person specifies that their data is to be used only for purpose, "A", after "A" has been achieved, it should be deleted. This limits the possibility of misuse. However in some instances the Government may prescribe mandatory data retention (call logs). (MyGov Link)

8. Individual Participation Rights - I (Pages 122-128)	Data protection requires practical enforcement of rights. Like asking who holds how much data on you. Also, people also have the right to ensure that data related to them is kept accurately as it may be used to offer and also to deny them services (insurance, or loans). (MyGov Link)
9. Individual Participation Rights - II (Pages 129-136)	Further rights include objecting to the collection of data, its analysis and disclosure. One more important right is, "data portability", which allows you to take your data from one platform to another (export your email contacts from GMail to Outlook). (MyGov Link)
10. Right to be forgotten (Pages 137-142)	Users sometimes reveal information publicly which is used by search engines but they lose the ability to remove it. This information may become embarrassing in time some may like to be forgotten by having a legal right for it's removal. (MyGov Link)

Part IV: Regulation and Enforcement

Part IV is titled "Regulation and Enforcement", and deals with the nuts and bolts of a proposed data protection regime. In particular, it addresses questions about how the entities that process your data might be regulated, what an accountability mechanism might look like in case they breach their obligations, and how you might be able to exercise your remedies in such cases. A summary of the four chapters in Part IV with key concepts which are outlined in a table below.

1. Enforcement models (Pages 143-146)	The enforcement of a data protection law requires a data protection authority that operates a regulator. For specific industries a co-regulatory model which allows industry bodies and sectors to define voluntary codes may promote higher compliance. (MyGov Link)
2. Accountability / Enforcement tools (Pages 147-182)	Given that consent and notice are not perfect safeguards additional protection is provided by a legal framework of data protection that emphasises of accountability of data controllers. This requires businesses and government to follow "privacy by design" in which external legal requirements are internally implemented. The accountability tool-kit includes, codes of practice (prescribed for employees handling data), data breach notifications, data audits and monitoring by a data protection authority which has powers of investigation and enforcement. (MyGov Link)
3. Adjudication Process (Pages 184-189)	The Information Technology Act has for years provided a limited protection of compensation for data breaches which has been unenforceable. This is not only because the protection was inadequate, but the body and process to enforce it was defective. Hence, how should a specialised body which can expertly apply issues of data protection enforce the remedies under it. (MyGov Link)

4. Remedies (Pages 191-203)	Remedies will include financial fines to deter negligence (weak securite leading to data breaches) and noncompliance (wilful overcollection of data) with data protection norms. Such remedies can be public remedies (fines for general breaches), or compensate specific harm to persons. This will require thresholds to be determined also whether such remedies will apply equally to private and government data controllers. Further, in some instances criminal offences may be necessary such as private information knowingly disclosed to cause significant harm to another person. (MyGov Link)

Summary : 7 Key Principles

Technology agnosticism	"The law must be technology agnostic. It must be flexible to take into account changing technologies and standards of compliance."
Holistic application	"The law must apply to both private sector entities and government. Differential obligations may be carved out in the law for certain legitimate state aims."
Informed consent	"Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. The law must ensure that consent meets the aforementioned criteria."
Data minimisation	"Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject."
Controller accountability	"The data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing."
Structured enforcement	"Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms."
Deterrent penalties	"Penalties on wrongful processing must be adequate to ensure deterrence."

Suggested readings

OECD Principles (link)
Necessary and Proportionate Principles (link)
Justice A.P. Shah Report on Privacy (link)
European Data Protection Regulation (link)