Dvara Research | Policy Brief | October 2019

Implementing the Personal Data Protection Bill:

Mapping Points of Action for Central Government and the future Data Protection Authority in India

Authors: Srikara Prasad, Malavika Raghavan, Beni Chugh & Anubhutie Singh[1]

Summary

The Central Government and the future Data Protection Authority (DPA) will face the complex task of notifying several rules and regulations in order to bring India's Personal Data Protection Bill (the Bill) into full effect. In the absence of such regulations, even if the Bill is enacted it could have limited impact and effect. There is a pressing need for a clear blueprint of how Central Government and the DPA will work together to systematically release regulation to bring to life the provisions of the Bill. A systematic approach could prevent the ad-hoc passage of rules which could create severe disruptions in the data economy and gaps in consumer protection.

In this policy brief, we set out the actions required from Central Government and the future DPA following enactment of the Bill. These actions are sequenced in order of priority based on our analysis of the interlinkages of sections within the Bill and the practical requirements of any data protection regime. The sequencing is aimed at ensuring that the main elements of the law come into effect without compromising consumer protections and inducing business uncertainty. This initial blueprint aims to drive forward the conversation on effective implementation, capacity and enforcement for India's future data protection regime taking into account our unique context.

[1] The authors work with Dvara Research, Mumbai, India. Our team benefitted from the intellectual engagement of Mr. Rahul Matthan throughout the development of this work. We thank him for his nuanced consideration of our views and rigorous peer review.

We welcome feedback and comments to refine our thinking. Comments welcome at FFI@dvara.com.

Introduction: Subordinate legislation under the draft Personal Data Protection Bill

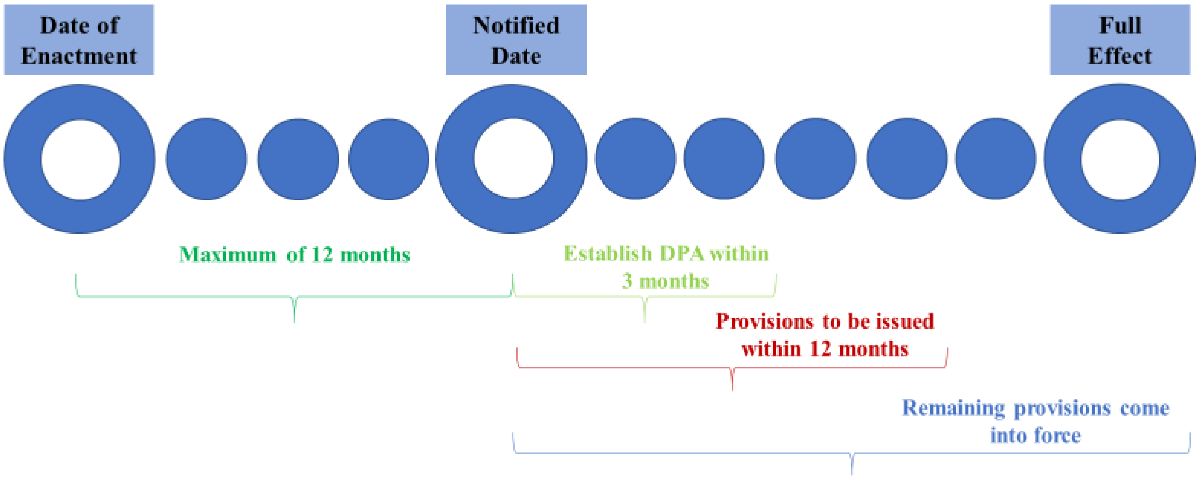
The draft Personal Data Protection Bill (the Bill) was released in July 2018 and followed by public consultation by the Ministry of Electronics and Information Technology (MeitY). If the Bill is passed by the Indian Parliament, it will result in the creation of an independent Data Protection Authority (DPA) entrusted with enforcing and overseeing the data protection regime in the country. The Central Government and the future DPA would then face the complex task of notifying several subordinate rules and regulations in order to bring the Bill into full effect.

This rule-making is critical for the effectiveness of the new data protection regime since the draft Bill defers several key details to be fleshed out in future regulations of the DPA. In the absence of such regulations, even if the Bill is enacted, it could have limited impact and effect. There is a pressing need for a clear blueprint of how the Central Government and the DPA will work together to systematically release regulation to bring to life the provisions of the Bill.

Through this policy brief, we seek to set out the actions that will be required from Central Government and the future DPA following enactment of the draft Bill in order to give it full effect. They are sequenced in order of priority based on our analysis of the interlinkages of sections within the Bill and the practical requirements of any data protection regime. The sequencing is aimed at ensuring that the main elements of the law come into effect without compromising consumer protection and inducing business uncertainty.

An assessment of the timelines in the draft Bill reveals that subordinate regulations on the various aspects of data protection need to be issued by Central Government and the DPA within an outer limit of **two and a half years** from the date of the enactment of the draft Bill.[2] This is represented pictorially below and explained in Table 1.

Figure 1: Timelines for issuing subordinate legislation under the draft Bill


Date of Enactment
Notified Date
Full Effect
Maximum of 12 months
Establish DPA within 3 months
Provisions to be issued within 12 months
Remaining provisions come into force

[2] S.97, (Chapter XIV- Transitional provisions), The Personal Data Protection Bill, 2018.

Section I of this brief summarises some of the timelines indicated in the draft Data Protection Bill 2018. Section II sets out the actions of the Central Government that need to be performed in the period between enactment of the law and from three months of the notified date. Section III sets out the actions that the DPA must perform following its establishment.

I. Timelines for implementation under the draft Personal Data Protection Bill

The key milestones and time periods (represented pictorially on page 1) to bring the future data protection law into force are summarized in the table below, as per section 97 of the draft Bill.

Table 1: Timelines for regulation-making under the draft Bill

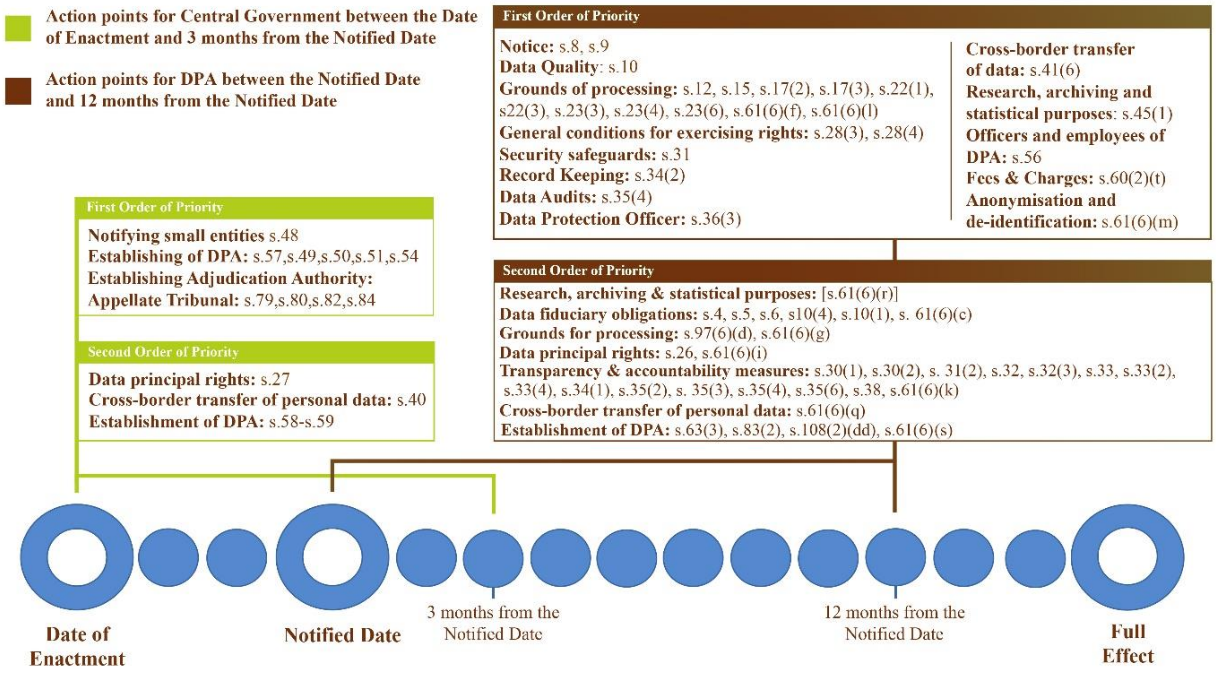
Milestone	Time period	Action for DPA/ Central Government in this time period
Date of enactment	Date on which the Act receives presidential assent.	The Central Government must specify a "notified date".
Notified date	Date notified by the Central Government in the Official Gazette within 12 months of the date of enactment.	The following provisions take effect on the notified date: - transitional provisions (under Chapter XIV); - provisions to enable the operation of the DPA (Chapter X); - the Central Government's power to make rules and the & DPA's powers to make regulations (respectively) under the draft Bill.
Establishment of the DPA	Within 3 months from the notified date	Central government must establish the DPA.
	Within 12 months from the notified date	The DPA must issue regulations on: - issuing codes of practice on different matters;[3] - grounds of processing personal data for reasonable purposes (s 17).[4]
Full effect	Within 18 months from the notified date.	All remaining provisions automatically come into effect 18 months from the notified date.

From this table, it becomes clear that after the Date of Enactment of the Bill, immediate actions will be required from the Central Government to establish the DPA, and subsequently to clarify the content of particular provisions. The DPA will also need to undertake a range of actions in the first 12 – 18 months of its establishment to give effect to the provisions of the Act.

[3] The Personal Data Protection Bill, 2018, s.97(6).
[4] The Personal Data Protection Bill, 2018, s.97(5).

This policy brief provides a blueprint of action points for the Central Government and the DPA to issue subordinate legislation. The blueprint is summarised in figure 2, which mentions all the rules and regulations which must be issued by the Central Government and the DPA. They are sequenced from left to right beginning at "Date of Enactment" and ending at "Full Effect." The segment colour-coded in light green contains all the action points for the Central Government, which must be completed between the Date of Enactment and 3 months from the Notified Date. The segment colour-coded in brown contains all the action points for the DPA, which must be completed between the Notified Date and 12 months from the Notified Date.

Figure 2: Blueprint for issuing subordinate legislation by the Central Government & the DPA in India



🟩 **Action points for Central Government between the Date of Enactment and 3 months from the Notified Date**

🟫 **Action points for DPA between the Notified Date and 12 months from the Notified Date**

First Order of Priority

Notifying small entities s.48
Establishing of DPA: s.57,s.49,s.50,s.51,s.54
Establishing Adjudication Authority:
Appellate Tribunal: s.79,s.80,s.82,s.84

Second Order of Priority

Data principal rights: s.27
Cross-border transfer of personal data: s.40
Establishment of DPA: s.58-s.59

First Order of Priority

Notice: s.8, s.9
Data Quality: s.10
Grounds of processing: s.12, s.15, s.17(2), s.17(3), s.22(1), s22(3), s.23(3), s.23(4), s.23(6), s.61(6)(f), s.61(6)(l)
General conditions for exercising rights: s.28(3), s.28(4)
Security safeguards: s.31
Record Keeping: s.34(2)
Data Audits: s.35(4)
Data Protection Officer: s.36(3)
Cross-border transfer of data: s.41(6)
Research, archiving and statistical purposes: s.45(1)
Officers and employees of DPA: s.56
Fees & Charges: s.60(2)(t)
Anonymisation and de-identification: s.61(6)(m)

Second Order of Priority

Research, archiving & statistical purposes: [s.61(6)(r)]
Data fiduciary obligations: s.4, s.5, s.6, s10(4), s.10(1), s. 61(6)(c)
Grounds for processing: s.97(6)(d), s.61(6)(g)
Data principal rights: s.26, s.61(6)(i)
Transparency & accountability measures: s.30(1), s.30(2), s. 31(2), s.32, s.32(3), s.33, s.33(2), s.33(4), s.34(1), s.35(2), s. 35(3), s.35(4), s.35(6), s.38, s.61(6)(k)
Cross-border transfer of personal data: s.61(6)(q)
Establishment of DPA: s.63(3), s.83(2), s.108(2)(dd), s.61(6)(s)

Date of Enactment
Notified Date
3 months from the Notified Date
12 months from the Notified Date
Full Effect

The blueprint has been created after analyzing requirements of the draft Bill and the practicalities of implementation. The action points in the blueprint are sequenced into (A) first order of priority and (B) second order of priority for the Central Government and the DPA separately based on:

- particular provisions of the Bill which need subordinate regulation to take effect;
- consumer protection considerations and the need to have effective user rights after the date of enactment of the Bill;
- practical clarity required by data fiduciaries and controllers to comply with obligations under the Bill.

The blueprint does not attempt to provide a step-by-step process for issuing subordinate legislation but broadly highlights the order in which subordinate legislation may be issued. Section II and section III explain these action points in detail by highlighting the precise actions required from the Central Government and the DPA to systematically bring the Bill into full effect.

II. Subordinate legislation to be issued by the Central Government

The draft Bill tasks the Central Government to make **rules** (under section 107) and **notifications** (under different provisions). The powers and functions of the Data Protection Authority (DPA) are reliant on the issuing of rules by the Central Government. Certain key substantive provisions also require implementing rules to be issued by the Central Government. Central Government thus needs to begin taking action immediately from the Date of Enactment of the Bill. In the tables below we set out the rules and notifications required to be issued, sequenced as (A) first order of priority and (B) second order of priority to facilitate a smooth transition and implementation of the future Personal Data Protection Act.

A. Central Government – First Order of Priority[5]

Subject	Action Point	Tool
Scope & Limitations	**Manual processing by small entities [s.48(2)(2)]:** Prescribing the amount of annual turnover of an entity for it to qualify as a small entity	Rule [s.107(2)(f)]
Establishment of DPA	**Grants by the Central Government [s.57]:** Specifying the sums of money to be given to the DPA as thought fit for the purpose of this legislation	Provision [s.57]
	Incorporation of the DPA [s.49]: Notifying the place of establishment, location of the head office of the DPA	Rule [s.107(2)(g)] Notification [s.49(1)]
	Appointment of DPA members [s.50]: Prescribing the composition and the qualifications of the DPA members	Rule [s.107(2)(h)]
	Terms and conditions of appointment [s.51]: Specifying the terms and conditions for service of DPA chairperson and members, and their remuneration	Rule [s.107(2)(i)]
	Meetings of the DPA members [s.54]: Specifying the times and places, rules and procedures for meetings of the DPA	Rule [s.107(2)(j)]
Establishment of DPA – Adjudication Authority	**Appointment of an Adjudicating Officer [s.68]:** Specifying the qualification, manner, terms and conditions of appointment and jurisdiction of the Adjudicating Officer	Rules [s.107(2)(u)] and [s.107(2)(v)]
	Manner of adjudication [s.74]: Specifying the manner in which adjudicating officers will conduct an inquiry	Rule [s.107(2)(w)]
	Manner of filing a complaint with the Adjudication Wing [s.39(4)]: Prescription of the manner in which a Data Principal may file a complaint for grievance redressal	Rule [s.107(2)(c)]

[5] As per s. 97(3), matters relating to Chapter X and s.107 will come into force on the notified date i.e. 12 months from the Bill's enactment. Therefore, the Central Government must deal with these matters as a priority.

	Manner of complaint and compensation to Data Principal after adjudication [s.75(2)]: Prescribing the form and manner in which a complaint may be instituted for adjudication and the compensation that may be offered	Rules [s.107(2)(x)] and [s.107(2)(y)]
	Codes of Practice [s.61]: Prescribing the procedure for issuing of Codes of Practice, the manner in which they may be modified or revoked and the manner in which they may be recorded	Rules under 107(2)(q), 107(2)(r) & 107(2)(s)
Appellate Tribunal	**Establishment of the Appellate Tribunal [s.79(1), s.80, s.82]:** Establishing an Appellate Tribunal, criteria for appointment and composition of the Tribunal, staff and their renumeration	Rules [s.107(2)(z)], [s.107(2)(aa)] & [s.107(2)(bb)]
	Appeals to the Appellate Tribunal [s.84]: Prescribing the form, manner and fee for filing an appeal or application before Appellate Tribunal	Rule [s.107(2)(cc)

B. Central Government – Second order of priority		
Subject	**Action Point**	**Tool**
Rights of Data Principals	**Right to be Forgotten [s.27(4)]:** Prescribing the manner and form for the application for exercising the Right to be Forgotten by Data Principals	Rule [s.107(2)(a)]
	Right to be Forgotten [s.27(5)]: Prescribing the manner in which orders of the Adjudicating officers may be applied for review with respect to the exercise of the right	Rule [s.107(2)(b)]
Cross-border transfer of personal data	**Conditions for cross-border transfer [s.41(1)(b)]:** Specifying of countries, or sector of countries or international organisations to which transfer of personal data is permissible	Rule [s.107(2)(d)]
	Conditions for cross-border transfer [s.41(4)]: Specifying the time period within which the DPA would be notified of cross-border transfer of personal data for emergencies under [s.41(3)]	Rule [s.107(2)(e)]
	Notification of Critical Personal Data [s.40(2)]: Notifying the categories of personal data as *critical personal data* that may only be processed within India	Notification [s.40(2)]
Establishment of the DPA	**Accounts and Audits [s.58]:** Prescribing the form in which accounts and annual statements will be recorded and the time intervals of account auditing of the DPA	Rule [s.107(2)(k)] and [s.107(2)(l)]
	Furnishing of returns, etc. to the Central Government [s.59]: Prescribing the form and manner in which returns, statements and particulars must be furnished to the Central Government	Rule [s.107(2)(m)]

III. Subordinate legislation to be issued by the Data Protection Authority

Most of the substantive provisions in the draft Bill need clear regulations and codes to be enacted by the future DPA to take effect. The draft Bill enables the DPA to issue **regulations** (under section 108), **notifications** (under different provisions) and **codes of practices** (under section 61) to strengthen and smoothen regulation under the future of data protection regime. Below we set out the actions to be taken by the DPA sequenced by those that need to be (A) first order of priority and (B) second order of priority, to give effect to the substantive provisions of the draft Bill.

A. DPA - First Order of Priority		
Subject	**Action Point**	**Tool**
Scope & Limitations	**Anonymisation [s.3(3)] and De-identification [s.3(16)]:** Providing methods of anonymisation and de-identification.	Codes of Practice [s.61(6)(m)]
	Research, Archiving or Statistical Purposes [s.45(1)]: Specifying the provisions which are not applicable to the processing of data for research, archiving or statistical purposes.	Regulations [s.108(2)9(z)]
Data Fiduciary Obligations	**Notice [s.8]:** Prescribing information which data fiduciaries must provide in notices.	Regulations [s.108(2)(a)]
	Notice [s.8]: Issuing model forms and guidance.	Codes of Practice [s.61(6)(a)]
	Data Quality [s.9]: Prescribing measures for ensuring data quality.	Codes of Practice [s.61(6)(b)]
Grounds of Processing	**Processing on the basis of consent [s.12]:** Prescribing conditions for valid consent.	Codes of Practice [s.61(6)(d)]
	Processing necessary for prompt action [s.15]: Prescribing measures for processing data on this ground.	Codes of Practice [s.61(6)(e)]
	Processing for reasonable purposes [s.17(2)]: Specifying reasonable purposes for which personal data can be processed.	Regulations [s.108(2)(c)] Notifications [s.97(5)]
	Processing for reasonable purposes [s.17(3)]: Prescribing safeguards to protect the rights of data principals.	Regulations [s.108(2)(d)]
	Processing for reasonable purposes [s.17(3)]: Specifying provisions of *Notice (s.8)* which are not applicable.	
	Issuing codes of practice for activities for which personal data can be processed on this ground.	Codes of Practice [s.61(6)(f)]
	Further categories of sensitive personal data [s.22(1)]: Prescribing further categories of sensitive personal data and the grounds on which these categories of data can be processed.	Regulations [s.108(2)(e)]

	Further categories of sensitive personal data [s.22(3)]: Prescribing additional safeguards for categories of personal data collected for repeated, continuous or systematic collection for profiling.	Regulations [s.108(2)(f)]
	Processing children's data [s.23(3)]: Prescribing factors for determining the appropriateness of age verification mechanisms.	Regulations [s.108(2)(g)]
	Processing children's data [s.23(4)]: Notifying guardian data fiduciaries.	Notifications [s.23(4)]
	Processing children's data [s.23(6)]: Specifying modifications in the activities of guardian data fiduciaries who offer counselling or child protection services.	Regulations [s.108(2)(h)]
	Issuing codes of practice for processing of personal data of children and development of appropriate age-verification mechanisms and mechanisms for processing data on the basis of consent of users incapable of providing valid consent.	Codes of Practice [s.61(6)(h)]
Rights of Data Principals	**General Conditions for Exercising Rights [s.28(3)]:** Prescribing the time period within which a data fiduciary must comply with a data principal's request.	Regulations [s.108(2)(i)]
	General Conditions for Exercising Rights [s.28(4)]: Prescribing the time period & manner in which a data fiduciary must convey reasons for refusing the request and inform data principal about the right to file a complaint with the DPA.	Regulations [s.108(2)(j)]
Transparency & Accountability Measures	**Security Safeguards [s.31(1)]:** Prescribing standards for security safeguards to be maintained by data fiduciaries and data processors.	Codes of Practice [s.61(6)(l)]
	Record-Keeping [s.34(2)]: Prescribing the form in should records will be maintained by data fiduciaries.	Regulations [s.108(2)(r)]
	Data Audits [s.35(4)]: Prescribing eligibility, qualifications and functions of data auditors.	Regulations [s.108(2)(v)]
	Data Protection Officer [s.36(3)]: Prescribing eligibility and qualifications for data protection officers.	Regulations [s.108(2)(w)]
Cross-Border Transfer of Personal Data	**Conditions for cross-border transfer [s.41(6)]:** Prescribing the manner of certification and time period within which transfer of data under standard contractual clauses and intra-group schemes.	Regulations [s.108(2)(y)]
Establishment of the DPA	**Officers and employees of DPA [s.56(1)]:** Appointing officers, employees, consultants and experts.	Regulations [s.108(2)(aa)]
	Officers and employees of DPA [s.56(2)]: Prescribing remuneration, salary or allowances, terms and conditions of services.	
	Fees & Charges [s.60(2)(t)]: Prescribing fees and charges for carrying out purposes of the Act.	Regulations [s.108(2)(bb)]

B. DPA - Second Order of Priority		
Subject	**Action Point**	**Tool**
Scope & Limitations	Issuing codes of practice for processing personal data/sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes.	Codes of Practice [s.61(6)(r)]
Data Fiduciary Obligations	**Fair and reasonable processing [s.4]:** Providing guidance on what the DPA interprets as *fair and reasonable*.	Informal Guidance
	Purpose limitation [s.5]: Providing guidance on what the DPA interprets as *reasonable* and *incidental purpose*.	Informal Guidance
	Collection Limitation [s.6]: Providing guidance on what the DPA interprets as *necessary for purposes of processing*.	Informal Guidance
	Data storage limitation [s.10(4)]: Prescribing the manner in which data must be deleted.	Regulations [s.108(2)(b)]
	Data storage limitation [s.10(1)]: Prescribing the measures pertaining to data retention.	Codes of Practice [s.61(6)(c)]
	Prescribing the methods of destruction, deletion or erasure of data when required under the Act.	Codes of Practice [s.61(6)(c)]
Grounds for Processing	Issuing codes of practice for processing of personal data under Chapter III.	Codes of Practice [s.97(6)(d)]
	Issuing codes of practice for processing of sensitive personal data under Chapter IV.	Codes of Practice [s.61(6)(g)]
Rights of Data Principals	**Right to data portability [s.26]:** Prescribing standards and means to avail the right to data portability.	Codes of Practice [s.61(6)(j)]
	Issuing codes of practice for exercise of any right by data principals.	Codes of Practice [s.61(6)(i)]
Transparency & Accountability Measures	**Transparency [s.30(1)]:** Prescribing the form in which data fiduciaries must make information available to data principals.	Regulations [s.108(2)(k)]
	Transparency [s.30(2)]: Prescribing the manner in which the data fiduciary must notify data principals of important operations in the processing of personal data.	Regulations [s.108(2)(l)]
	Security safeguards [s.31(2)]: Prescribing the manner in which security safeguards must be periodically reviewed.	Regulations [s.108(2)(m)]
	Personal data breach [s.32(3)]: Prescribing the time period within which the data fiduciary must issue personal data breach notification to the DPA.	Regulation [s.32(3)]

Transparency & Accountability Measures	**Personal data breach [s.32]:** Prescribing the appropriate action to be taken in response to a personal data breach.	Codes of Practice [s.61(6)(o)]
	Data Protection Impact Assessment [s.33(2)]: Specifying the circumstances or classes of data fiduciaries or processing operations for which it is mandatory to conduct a Data Protection Impact Assessment.	Regulations [s.108(2)(n)]
	Data Protection Impact Assessment [s.33(2)]: Specifying the cases where the Data Protection Impact Assessment must engage a Data Auditor.	Regulations [s.108(2)(o)]
	Data Protection Impact Assessment [s.33(4)]: Prescribing the manner in which the DPIA report must be submitted to the DPA.	Regulations [s.108(2)(p)]
	Data Protection Impact Assessment [s.33]: Prescribing the manner in which DPIA must be carried out.	Codes of Practice [s.61(6)(p)]
	Record-keeping [s.34(1)]: Prescribing *other aspects of processing* for which records must be maintained.	Regulations [s.108(2)(q)]
	Record-keeping [s.34(1)]: Providing guidance on what the DPA interprets as *important operations in the data life-cycle*.	Informal Guidance
	Data Audits [s.35(2)]: Prescribing the factors which must be considered while evaluating compliance with stated provisions.	Regulations [s.108(2)(s)]
	Data Audits [s.35(2)(f)]: Prescribing the other matters with which data fiduciary's compliance should be evaluated.	Regulations [s.35(2)(f)]
	Data Audits [s.35(3)]: Prescribing the form, manner and procedure by which data audits must be conducted.	Regulations [s.108(2)(t)]
	Data Audits [s.35(6)]: Prescribing the criteria which will be used for rating data trust scores.	Regulations [s.108(2)(u)]
	Data Audits [s.35(4)]: Registering persons as data auditors.	Regulations [s.35(4)]
	Classification as significant data fiduciaries [s.38(1)]: Notifying certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries.	Notifications [s.38(1)]
	Classification as significant data fiduciaries [s.38(2)]: Prescribing the manner in which significant data fiduciaries must register themselves with the DPA.	Regulations [s.108(2)(x)]
	Classification as significant data fiduciaries [s.38(3) & s.38(4)]: Notifying the obligations which will apply to different classes or kinds of data fiduciaries.	Notifications [s.38(3) & s.38(4)]
	Prescribing measures for transparency and accountability, including standards to be maintained by data fiduciaries and data processors under Chapter VII.	Codes of Practice [s.61(6)(k)]
Cross-Border Transfer of Personal Data	Issuing codes of practice for cross-border transfer of personal data under section 41.	Codes of Practice [s. 61(6)(q)]

Establishment of the DPA	**Power to call for information [s.63(3)]:** Prescribing manner in which information shall be provided to the DPA.	Regulations [s.108(2)(cc)]
	Distribution of business amongst benches [s.83(2)]: Notifying distribution of the business of the Appellate Tribunal among benches, transfer of members between benches and provide for matters which may be dealt with by each bench	Notification [s.83(2)]
	Issuing rules and regulations in any other matter which the DPA views as required.	Regulations [s.108(2)(dd)]
		Codes of Practice [s.61(6)(s)]

Contact Us

Dvara Research, Chennai
10th Floor-Phase 1,
IIT-Madras Research Park,
Kanagam Village, Taramani
Chennai 600113

Dvara Research, Mumbai
The Mosaic, Raaj Chambers, 5th Floor,
New Nagardas Road,
Modra Pada, Andheri (E)
Mumbai 400053

E-mail: ffi@dvara.com

Twitter: @dvararesearch

@_FutureFinance

Website: www.dvara.com/research/