Divergence between the General Data Protection Regulation and the Personal Data Protection Bill, 2019

20 February, 2020

By **Pallavi Bedi**
Edited by **Amber Sinha**

The Centre for Internet and Society, India

Introduction

The European Union's General Data Protection Regulation (**GDPR**), replacing the 1995 EU Data Protection Directive came into effect in May 2018. It harmonises the data protection regulations across the European Union. In India, the Ministry of Electronics and Information Technology had constituted a Committee of Experts (chaired by Justice Srikrishna) to frame recommendations for a data protection framework in India. The Committee submitted its report and a draft Personal Data Protection Bill in July 2018 (**2018 Bill**). Public comments were sought on the bill till October 2018. The Central Government revised the Bill and introduced the revised version of the Personal Data Protection Bill (PDP Bill) on December 11, 2019 in the Lok Sabha.

The PDP Bill has incorporated certain aspects of the GDPR, such as requirements for notice to be given to the data principal, consent for processing of data, establishment of a data protection authority, etc. However, there are also areas of divergence between the two. The table below compares the provisions of the GDPR with the PDP Bill in their respective columns and highlights the significant changes in the comments column. We have only included provisions/terms which are common to the GDPR and the PDP Bill. It does not include the provisions on (i) Appellate Tribunal, (ii) Finance, Account and Audit; and (iii) Non- Personal Data.

In this note, we have used the term controller and data subject for the purpose of GDPR and data fiduciary and data principal for the purpose of the PDP Bill.

1. Scope

Jurisdiction

GDPR

Extends to all govt and private legal entities and individuals established in the EU or outside the EU and offering goods or services to EU residents.[1]

PDP Bill

- Applies to processing of personal data by the State, private entity or any individual, where such data has been collected, stored, shared or otherwise processed in India.[2]
- Processing of data by persons, companies not present within the territory of India, if such processing of data is (a) in connection with any business carried out in India, or any systematic activity of offering goods or services to persons in India; or (b) in connection with any activity which involves profiling of data of data principals within India.

The GDPR and the PDP Bill provide for extraterritorial application of the law.

Anonymised data

GDPR

Processing of anonymised data is excluded from the ambit of GDPR.[3]

PDP Bill

Processing of anonymised data is outside the ambit of the PDP Bill, other than the anonymised data referred to in Clause 91.[4]

1 Article 3
2 Clause 2(A)
3 Article 2 (1)
4 Clause 2(B)

2. Definitions

Personal Data

GDPR

Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[5].

PDP Bill

Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline or any combination of such features, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.[6]

Wider definition under the GDPR- It recognises identifiers such as location data, online identifiers as independently capable of identifying a natural person. It does not qualify the scope of such personal data with the terms 'any characteristic, trait, attribute or any other feature of the identity' as used by the PDP Bill.

Profiling

GDPR

Any form of **automated processing** of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

PDP Bill

Any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interest of a data principal.

PDP Bill recognises both manual as well as automatic processing of data.

5 Article 4(1)

6 Clause 3(28)

Anonymisation/ pseudonymisation

GDPR

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

PDP Bill

Anonymisation means the **irreversible process of** transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards of irreversibility specified by the Data Protection Authority.

GDPR does not mandate an irreversible process of anonymisation- which may not be possible and also does not take into account advancement in technology.

Sensitive personal data

GDPR

Not separately defined.

Article 9 states that processing of special kind of personal data is prohibited. Namely, data relating to (i) racial or ethnic origin, (ii) political opinions, (iii) religious or philosophical beliefs, (iv) trade union membership, (v) processing of genetic data, (vi) biometric data for the purpose of uniquely identifying a natural person, data concerning health , or (vii) data concerning a natural person's sex life or sexual orientation

PDP Bill

Personal data, which may, reveal, be related to, or constitute

(i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or politica belief or affiliation; or (xii) any other data categorised as sensitive personal data.

3. Obligations of Data Fiduciary

Processing of Personal Data

GDPR	PDP Bill
To be processed in a lawful, fair and transparent manner[7]	To be processed in a fair and reasonable manner and ensure the privacy of the data principal.[8]

The PDP Bill is silent on the processing of personal data to be done in a transparent manner.

Purpose Limitation

GDPR	PDP Bill
Collected only for specified, explicit and legitimate purpose and no further processing in a manner that is incompatible with those purposes[9]	No personal data shall be processed by any person, except for specific, clear and lawful purpose.[10] Further, it is to be processed only for purposes consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect such personal data shall be used for, having regard to the purpose and for the context and circumstances in which the personal data was collected.[11]

7 Article 5(1) (a)
8 Clause 5(a)
9 Article 5 (1)(b)
10 Clause 4
11 Clause 5(b)

As per GDPR, personal data may only be collected for specified legitimate purposes whereas, under the PDP Bill, data may be processed (which includes collection, recording, organisation, structuring, storage, alteration etc) for specified legitimate purposes.

The GDPR uses the 'compatibility' test, i,e whether the further processing of data is compatible with the original purpose for which the data was collected to determine the validity of such further processing.

The PDP bill permits incidental processing of personal data. Incidental purpose is a wider standard than the compatibility test.

Collection Limitation (data minimisation)

GDPR	PDP Bill
Personal data to be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed[12]	Collection of personal data limited to such data that is necessary for the purpose of processing.[13]

Wider ambit for collection of personal data under the GDPR- circumscribed by adequacy, relevance and necessity of the data.

Accuracy of personal data

GDPR	PDP Bill
Personal Data to be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that the personal data that are inaccurate are erased or rectified without delay.[14]	Data Fiduciary to take necessary steps to ensure that the personal data that is processed is complete, accurate, and not misleading and updated, having regard to the purposes for which it is processed.[15]

12 Article 5(1)
13 Clause 6
14 Article 5(1)(d)
15 Clause 8(1)

Data Storage Limitation

GDPR	PDP Bill
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are necessary.[16] It may be processed for longer periods in so far as the personal data will be processed solely for achieving purposes in public interest, scientific or historical research purposes.	Personal Data not to be retained beyond the period necessary to satisfy the purpose for which it was processed.[17] It may be retained for a longer period of time if such retention is explicitly consented to by the data principal, or necessary to comply with any obligation under a law.[18]

The GDPR explicitly specifies the grounds for which the personal data may be retained for a longer period.

3A. Notice/Information to be provided to the data principal

The GDPR and the PDP Bill provide comprehensive categories of information to be provided to the data principal such as the purpose for which the personal data is to be processed, the categories of personal data to be collected; contact details of the Data Protection Officer etc. However, there are also areas of divergence and these have been highlighted in the table below:

Automated Decision making

GDPR	PDP Bill
The controller shall inform the data subject about the existence of an automated decision making including profiling.[19]	No corresponding provision. It does not give the citizen the right to object to profiling, except in the cases of children.[20]

Under the PDP Bill, the data principal should have the right to be informed about the existence of an automated decision making including profiling.

16 Article 5(1)(e)
17 Clause 9(1)
18 Clause 9(2)
19 Article 13(2)(f)
20 Clause 16(5)

Right to seek rectification /correction

GDPR	PDP Bill
Data subject has the right to obtain without undue delay, rectification of inaccurate personal data. She also has the right to have the incomplete personal data completed.[21]	Data principal shall where necessary, having regard to the purposes for which the personal data has been processed, has the right to seek[22] (a) correction of inaccurate or misleading personal data; (b) completion of personal data; (c) updating of personal data

The GDPR unlike the PDP Bill does not provide the data principal the explicit right to seek the updation of personal data. Further, under the GDPR, the rectification has to be undertaken without undue delay- no time period has been specified under the PDP Bill.

Time limit for providing information when data not collected from the data subject

GDPR	PDP Bill
In case the personal data has not been collected from the data subject, the controller is required to provide the information latest within one month from the date of obtaining the personal data[23].	No time period has been prescribed under the Bill. It states that if the personal data has not been collected from the data principal, the information shall be provided as soon as reasonably practicable.[24]

21 Article 16

22 Clause 18

23 Article 14 (3)- (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, latest at the time of the first communication to the data subject; (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

24 Clause 7(1)

Provision for processing of personal data

GDPR	PDP Bill
The controller is required to inform the data subject about whether processing of personal data is necessary for the performance of a contract and whether the data subject is obliged to provide the personal data, and the consequences of the failure to provide such data[25].	If the data principal withdraws consent for the processing of any personal data without any valid consent, all legal consequences for the effects of such withdrawal shall be borne by the data principal[26].

Under the PDP Bill, the data principal shall bear all the consequences of the withdrawal of consent. However, it does not provide any corresponding obligation on the data fiduciary to inform the data principal about the possible consequences at the time of collecting personal data.

25 Article 13 (2)(e)

26 Clause 11 (6)

4. Grounds for processing of personal data without consent

Consent is the primary ground for processing of personal data and sensitive personal data under both GDPR and the PDP Bill. But, both GDPR and PDP recognise the importance of specifying the grounds for non-consensual processing of personal data.

Function of State

GDPR	PDP Bill
No specific provision- provides for processing of personal data if it is **necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.**[27]	Personal data may be processed if such processing is necessary; (a) for the performance of any function of the State authorised by law for (i) the provision of any service or benefit to the data principal from the State; or (ii) the issuance of any certification, license or permit for any action or activity of the data principal by the State.[28]

Under the PDP Bill- the State has a much wider ambit to process personal data. No guidelines provided to restrict such power of the State. - It can process the personal data for 'any function' of either the Parliament or State Legislature.

Compliance with law or any order of court or tribunal

GDPR	PDP Bill
Processing is necessary for compliance with a legal obligation to which the controller is subject.[29]	Personal data may be processed if such processing is necessary under any law for the time being in force or for compliance with any order or judgement any court or tribunal in India[30]

The ambit for processing of such personal data under the particular ground is the same under both the regulations.

27 Article 6(1)(e)
28 Clause 12(1)(a)
29 Article 6 (1)(c)
30 Clause 12(c)

Necessary for prompt action

GDPR	PDP Bill
processing is necessary in order to protect the vital interests of the data subject or of another natural person.[31]	It may be processed if such processing is necessary— (a) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual[32]; (b) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health[33]; or (c) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.[34]

As per Recital 46 of the GDPR- vital interests of the data subject refers to processing when it is necessary to protect protect an interest which is essential for the life of the data subject or that of another natural person. It may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics.

31 Article 6(1)(d)
32 Clause 12(d)
33 Clause 12(e)
34 Clause 12(f)

Employment purposes

GDPR

Member states by law may provide the specific rules for processing of personal data for employment purposes. The rules should include suitable measures to safeguard the employee's human dignity and fundamental rights.[35]

PDP Bill

Personal Data not being sensitive personal data may be processed if it is necessary for (a) recruitment or termination of the employment of the data principal; (b) provision of any service sought by, the data principal who is an employee of the data fiduciary; (c) verifying the attendance of the employee or for assessing the performance of the employee.

The GDPR recognises the power asymmetry between the employer and the employee and therefore the focus of the regulations appears to be on protecting the rights of the employees.

35 Article 88 (1) and (2)

5. Personal and Sensitive Data of Children

Age for consent

GDPR	PDP Bill
16 years[36]	18 years[37]

Parental consent for processing

GDPR	PDP Bill
Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.[38] Member states may provide for a lower age provided that such age is not below 13 years. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.[39]	Parental or guardian's consent required for processing of any personal data of children.

36 Article 8(1)
37 Clause 3(8) read with Clause 16(2)
38 Article 8(1)
39 Article 8(2)

Manner of verification

GDPR	PDP Bill
Controller shall take all reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	Manner of verification of the age of the to be specified by regulations taking into consideration; the (a) volume of personal data processed; (b) the proportion of such personal data likely to be that of a child; © possibility of harm to child arising out of processing of personal data

Guardian Data Fiduciaries

GDPR	PDP Bill
	Data fiduciaries who operate commercial websites directed at children or who process large volume of personal data of children.[40] The Data Protection Authority shall notify such data fiduciaries as Guardian Data Fiduciaries.- barred from profiling, tracking, or behavioural monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.

GDPR does not have a separate category of data fiduciary with respect to children.

40 Clause 16(4)

6. Rights of Data Principal

Right to correction

GDPR	PDP Bill
The data subject shall have the right to obtain from the controller without undue delay[41] the rectification of inaccurate personal data concerning her.[42]	Where necessary and having regard to the purpose for which the personal data is being processed, the data principal has the right to seek correction of the data.[43]

The right to correction under the PDP Bill has been qualified by the words ' where necessary', having regard to the purpose for which the data is being processed. It further does not specify the time-period within which the data has to be rectified.

41 Article 12
42 Article 16
43 Clause 18(1)

Right to erasure and Right to be forgotten

GDPR

The data subject can seek the erasure of personal data and the controller will be under an obligation to do so if (a) data subject withdraws consent or (b) data subject objects to the processing or (c) the processing is no longer necessary to fulfil the purpose for it was collected, or (d) the personal data was unlawfully processed; or (e)it has to be erased for compliance with a legal obligation.[44]

PDP Bill

Data principal has the right to seek the erasure of her personal data which is no longer necessary for the purpose for which it was processed.

The data principal has the right to restrict or prevent continuing disclosure of personal data by the data fiduciary. This will be applicable if the Adjudicating Authority determines that the data disclosure is no longer necessary, or where the processing of personal data is based on the consent of the data principal, the consent to use data has been withdrawn or the data is being used contrary to the provisions of the law, and that the rights and interests of the data principal override the right of freedom of expression and the right to information of any citizen.[45]

The GDPR has combined the right to erasure and the right to be forgotten under one provision

The PDP Bill does not specify any conditions for the data principal to be able to exercise such a right. (though the conditions may be specified in the regulations). The data fiduciary can reject such a request provided it gives an adequate justification for doing so.

Right to erasure is a new right introduced in the 2019 Bill- it wasn't provided for under the 2018 Bill.

The provision under the PDP Bill does not provide for the right to be forgotten, it is instead a Right to seek Restriction on Processing of Personal Data.

GDPR incorporates a more extensive right to be forgotten, and imposes a requirement on data controllers to erase any data pertaining to the data subject when such erasure is requested under an appropriate ground. Data controllers can, however, refuse to erase personal data relying on alternative legal bases, such as compliance with law or further to a legitimate business interest23.

Under the PDP Bill, the proposed right is subject to the approval of the Adjudicating Authority constituted under the Bill; which is not the case under the GDPR.

44 Article 17

45 Clause 20(2)

Right to confirmation and access

GDPR

The data principal has the right to obtain information from the controller whether the personal data has been processed.[46]

The information shall be provided in a clear a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

PDP Bill

The data principal has the right to obtain from the data fiduciary (a) confirmation whether the data fiduciary is processing or has processed personal data; (b) a brief summary of the personal data of the data principal being processed or that has been processed by the data fiduciary; (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice to be provided to the data principal.[47]

Data principal has the right to access in one place the identities of the data fiduciaries with whom her personal data has been shared.

The data fiduciary shall provide the information to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person.[48]

The language under the PDP Bill appears to be broader; the data principal has the right to know whether the personal data has been processed or is being processed, whereas under the GDPR the information is limited to whether personal data has been processed.

Further, under the PDP Bill, the data principal can access the identities of all the other data fiduciaries with whom the data has been shared in one place- no corresponding right under the GDPR.

46 Article 15(1)
47 Clause 17(1)
48 Clause 17 (2)

Right to restriction of processing

GDPR	PDP Bill
Specifies the grounds under which the data principal has the right to restrict the data fiduciary from processing personal data[49]. These include; (a) contesting the accuracy of the personal data, for a period enabling the data fiduciary to verify the accuracy of the personal data; (b) unlawful processing and the data principal opposes the erasure of the personal data and requests the restriction of their use instead ; (c) the data fiduciary no longer needs the data for the purpose of processing, but they are required by the data principal for the establishment, exercise or defence of a legal claim; or (d) the data principal has objected to the processing of personal data.	Not explicitly provided though the Right to be Forgotten provides three grounds under which the data principal shall have the right to restrict or prevent continuing disclosure of personal data.

49 Article 18(1)

7. Transparency and Accountability Measures

A. Transparency and Accountability

Privacy by Design

GDPR	PDP Bill
The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR.[50]	Every data fiduciary shall implement policy measures to ensure managerial, organisational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data principal. Further, the policy should ensure that privacy is protected throughout processing from the point of collection to deletion of personal data.[51]

The scope of privacy by design under the PDP Bill appears wider than what has been provided under the GDPR. The Bill places an obligation on the data fiduciary to ensure that privacy is protected throughout processing from the point of collection to deletion of personal data, whereas the GDPR merely stipulates that the privacy mechanism should be implemented at the time of determining the means for processing and at the time of processing.

It does not cover the stage of deletion of personal data.

50 Article 25 (1)

51 Clause 22(1)

Privacy by default

GDPR	PDP Bill
The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility	No provision

Transparency

GDPR	PDP Bill
Controller is required to provide the relevant and necessary information[52] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.	Data Fiduciary to maintain transparency in processing personal data and has to provide certain details including information about the categories of personal data collected, purpose for which the data is processed, right of the data principal to file a complaint to the Data Protection Authority.[53] Data principal may give or withdraw consent through a consent manager.[54]

No specific provision about the use of consent managers by data principals under GDPR

52 Article 12 (1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

53 Clause 23(1)

54 Clause 23(3)

B. Security Safeguards

Who shall implement

GDPR	PDP Bill
Controller and Processor[55]	Data Fiduciary and Processor[56]

Conditions to be taken into account

GDPR

- Implementation cost;
- Nature, context and purpose of processing;
- Risks of varying likelihood; and
- Severity for the rights and freedom of natural persons

PDP Bill

- Nature, scope, context and purpose of processing;
- Risks associated with such processing; and
- likelihood and severity of the harm that may result from such processing

The focus of the GDPR is the effect of the processing on the rights and freedom of persons. Under the PDP Bill, the focus is on the severity of the 'harm' that may result from such processing.

The PDP Bill does not provide any guidelines on either the interpretation of the term 'harm,'[57] or on the various activities covered within the definition of the term. Terms such as 'loss of reputation or humiliation' 'any discriminatory treatment' are a subjective standard and are open to varied interpretations. Therefore, using harm as a measure to determine the security measures to be implemented may not provide any guidance on the measures to be adopted.

55 Article 32(1)

56 Clause 24(1)

57 Clause 3(20): "harm" includes (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (ii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of service,benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal.

Measures to be implemented

GDPR	PDP Bill
• Pseudonymisation and encryption of personal data; • Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; • Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; • Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	• De-identification and encryption; • Steps necessary to protect the integrity of personal data; • Steps necessary to prevent misuse, unauthorised access to, modification,disclosure or destruction of personal data

C. Personal Data Breach

Who should be notified

GDPR	PDP Bill
The Supervisory Authority[58]	The Data Protection Authority[59]

58 Article 33(1)

59 Clause 25(1)

When to notify

GDPR

Without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

PDP Bill

The Data Protection Authority is to be notified about the breach of personal data, when the breach is likely to cause harm to any data principal.

The information should be provided as soon as possible and if it is not possible to provide all the information at the same time, the information may be provided in a staggered manner.[60]

Communication to the data principal

GDPR

If the data breach is likely to result in a high risk to the rights and freedom of natural persons, then the controller is required to notify the data subject without any delay.[61]

PDP Bill

The Data Protection Authority has to determine whether the data fiduciary should notify the data principal about the breach. This will be done after taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.[62]

Under the PDP Bill, it is the Data Protection Authority who has been vested with the responsibility of determining whether the data principal should be notified about the breach. Under both the regulations, the data principal is not automatically notified about each breach of personal data. Communication to the data principal is based on the severity of the risks and the likelihood of the harm to be caused to the data principal.

60 Clause 25(3)
61 Article 34(1)
62 Clause 25(5)

D. Grievance Redressal

Right to lodge a complaint with the Authority

GDPR

The data subject has the right to lodge a complaint with the supervisory authority.[63]

PDP Bill

The data fiduciary is required to have a proper and effective system of grievance redressal in place[64]. The grievance has to be redressed in an expeditious manner in maximum 30 days from the date of receipt of the grievance by the data fiduciary.[65]

In the event the data principal is not satisfied with the way in which the dispute has been resolved by the data fiduciary, then she has the right to file a complaint with the adjudication wing of the Data Protection Authority.[66]

The PDP Bill envisages a two tier system for grievance redressal. The data principal cannot directly approach the Data Protection Authority, she has to first seek redress with the grievance redressal mechanism provided by the data fiduciary.

63 Article 77 (1)
64 Clause 32 (1)
65 Clause 32 (3)
66 Clause 32 (4)

E. Audit of policies and conduct of processing etc

Who shall conduct it

GDPR

Each Supervisory Authority shall have the power to carry out investigations in the form of data protection audits[67]

Through legislation enacted by member states to enforce the GDPR, Information Commissioners have also commenced conducting consensual data audits.

PDP Bill

Independent Data Auditor recognized and authorized by the Authority.[68] The Data Protection Authority shall register persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, with such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may specify, as data auditors.

The GDPR provides for data protection audit in the form of a coercive mechanism- however, the information commissioners established by member states have identified data audits in educating and assisting organisations to meet their obligations.

Applicability

GDPR

Any Controller/Processor

PDP Bill

Significant Data Fiduciaries.

The data fiduciary shall have policies in place for an annual data audit to be undertaken by the independent data auditor.

GDPR does not specify the controllers that are required to undertake a data audit. It also does not specify the time period for conducting the audit.

67 Article 58(1)(b)

68 Clause 29(1)

F. Data Protection Officer

Who should appoint a Data Protection Officer

GDPR

- Processing is carried out by a public authority
- Core activities of the controller requires regular and systematic monitoring of data subjects on a large scale
- Core activities of the controller requires processing on a large scale of special categories of data.[69]

A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

PDP Bill

Significant data fiduciaries[70] to appoint a Data Protection Officer.[71]

The Data Protection has to be based in India and shall represent the data fiduciary under the Bill[72]

Similar thresholds under both the laws- though, the ambit is wider under the PDP Bill (as it also takes into account the turnover of the data fiduciary and the risk of harm resulting from the processing).

GDPR does not specify that the Data Protection Officer has to be based in the country of the data fiduciary.

69 Article 37(1)

70 Clause 26 (1): The Authority shall having regard to the following factors, notify certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries— (a) volume of personal data processed; (b) sensitivity of personal data processed; (c) turnover of the data fiduciary; (d) risk of harm resulting from any processing or any kind of processing undertaken by the fiduciary; (e) use of new technologies for processing; and (f) any other factor relevant in causing harm to any data principal as a consequence of such processing.

71 Clause 30 (1) read with Clause 26 (1)

72 Clause 30 (3)

Responsibilities of the Data Protection Officer

GDPR

- Inform and advise the controller about their responsibilities and obligations under the GDPR.
- Monitor compliance with the regulation and the policies of the controller with respect to the processing of personal data.
- Provide advice as required as regards the data protection impact assessment.
- Cooperate with the supervisory authority
- Contact person for the for the supervisory authority on issues relating to processing

PDP Bill

- Provide information and advice to the data fiduciary on matters relating to fulfilling its obligations under the PDP Bill.
- Monitor the personal data processing to ensure it does not violate the PDP Bill.
- Provide advice to the data fiduciary where required on the manner in which data protection impact assessments must be carried out, and to carry out a review of such an assessment.
- Act as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary.
- Provide assistance to and cooperating with the Data Protection Authority on matters of compliance of the data fiduciary with provisions under the PDP Bill.[73]

Similar responsibilities under both the regulations.

Qualifications

GDPR

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks

PDP Bill

To be specified by the Central Government

73 Clause 30 (1)

G. Processing by entities other than the data fiduciary

Appointment of a processor

GDPR	PDP Bill
Processing by a processor shall be governed by a contract or other legal act that is binding on the processor with regard to the controller and that sets out the (a) subject-matter and duration of the processing, (b) the nature and purpose of the processing, (c) the type of personal data and categories of data subjects (d) and the obligations and rights of the controller.[74]	The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.[75]

The method of appointment of processor is similar. However, while the GDPR specifies the provisions of the contract, no information provided in the PDP Bill on the details to be provided in the contract between the data fiduciary and the processor.

Engagement of another processor

GDPR	PDP Bill
The processor shall not engage another processor without prior specific or general written authorisation of the controller[76].	The data processor shall not engage or appoint another data processor on its behalf, except with the authorisation of the controller.[77]

The method of appointment of processor is similar. However, while the GDPR specifies the provisions of the contract, no information provided in the PDP Bill on the details to be provided in the contract between the data fiduciary and the processor.

74 Article 28 (2)
75 Clause 31 (1)
76 Article 28 (2)
77 Clause 31(2)

8. Restrictions on transfer of personal data outside India

Restriction on transfer of data

GDPR	PDP Bill
Contains a clear bifurcation in regulation of data transfers to countries which have obtained an adequacy decision and to those that have not. In case of a failure of the adequacy decision, there are specific safeguards that need to be verified before data may be transferred to a country that is not deemed to be 'safe,' such as an enforceable instrument between the countries, standard contractual clauses or binding corporate rules	Sensitive personal data may be transferred outside India, subject to certain conditions,[78] but such sensitive personal data shall continue to be stored in India. Critical Personal Data (to be notified by the Central Government) shall only be processed in India.

78 Clause 33(1)

Condition for transfer

GDPR	PDP Bill
Personal data may be transferred to another country without a specific authorisation from the supervisory authority when the European Commission has decided that the country or one or more specified sectors within that country ensures an adequate level of protection.[79] In the absence of an adequacy decision by the EC, the controller may transfer data to another country only if the controller has provided appropriate safeguards.[80]	Sensitive personal data may only be transferred outside India, when explicit consent is given by the data principal[81]; and where a. The transfer is made pursuant to a contract or intra group scheme approved by the Data Protection Authority; b. Central Government in consultation with the Data Protection Authority has allowed the transfer to a country, or an international organisation that offers an adequate level of protection; c. The Data Protection Authority has permitted the transfer of any sensitive personal data for any specific purpose.

The GDPR does not have restrictions on the categories of personal data that may be transferred. The emphasis is on ensuring that the country to which the data is being transferred provided an adequate level of protection to the data subject, irrespective of the category of data that is being transferred.

Critical Personal Data

GDPR	PDP Bill
No provision	The Central Government shall notify certain categories of sensitive personal data as critical personal data. Such data shall only be processed in a server or data centre located in India.

79 Article 45 (1)
80 Article 46 (1)
81 Clause 34(1)

9. Exemptions

Power of the State to grant exemption

GDPR

A member state to which the data processor data fiduciary is subject to, may by way of a legislative measure restrict the rights of the data subject and the corresponding obligations of the controller provided under Article 12-22. Any such restriction should be necessary and proportionate to safeguard[82];

a. National security;

b. Defence;

c. Public security;

d. The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

e. Other important objectives in particular important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

f. Protection of judicial independence

g. Prevention, investigation, detection and prosecution of ethical breaches;

h. Monitoring , inspection, even occasionally to the exercise of official authority in points (a) to (e) and (g)

i. Protection of rights of data subject;

j. enforcement of civil law claims.

PDP Bill

The Central Government may by way of a written order direct that any or all of the provisions of the Bill will not apply to any agency of the Government, if it is satisfied that it is necessary or expedient (i) in the interest of sovereignty and integrity of India, the Security of the State, friendly relations with foreign States, public order; or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order.[83]

Where the personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law, such processing shall be exempt from complying with certain provisions of the Bill.[84]

82 Article 23(1)
83 Article 35
84 Article 36(a)

Any provision curtailing the right to privacy has to pass a three fold test; (i) should be authorised by law; (ii) legitimate state aim; and (iii) it should be proportionate to the interests sought to be achieved.

GDPR explicitly states that any measure restricting the right of the data subject has to be by way of a legislative measure and it has to be necessary and proportionate. Under the PDP, the exemption is conferred by way of a written order of the Central Government.

Unlike the PDP Bill, GDPR enumerates the specific grounds when such a measure may be undertaken.

The PDP Bill grants a blanket exemption from all the provisions of the Bill to an agency of the Central Government- it is not specific to a particular function or specific purpose of the particular agency.

With respect to the provision pertaining to granting exemption for the processing of personal data in the prevention, detection and investigation of offences; the GDPR specifies this is exemption is applicable to criminal offences or criminal penalties. The PDP Bill uses the term 'offence', there is no clarity on this term and therefore even a breach of a contractual clause could fall within this clause.

Oversight mechanism

GDPR	PDP Bill
The legislative measure should contain specific measures relating to the safeguards to prevent abuse or unlawful access, and also the right of the data subject to be informed about the restriction, unless that may be prejudicial to the purpose of the exemption.[85]	The procedure, safeguards and the oversight mechanism will be prescribed in the future.[86]

The PDP Bill delegates the oversight mechanism to the subordinate legislature. No oversight mechanism prescribed in the PDP Bill.

85 Article 23(2)

86 Clause 35

10. Data Protection Authority

The GDPR proposes the establishment of a Supervisory Authority by each Member State to monitor the application of the regulations. Each Member State shall by law provide the qualifications, the rules for appointment of the members and the duration of term for each member.

Establishment of an Authority

GDPR	PDP Bill
Each member state to provide for one or more independent public authority (supervisory authority) to monitor the application of the regulation.[87]	Central Government to establish a Data Protection Authority[88]

Under the GDPR, Member States are free to establish one or more supervisory authorities. Currently, the PDP Bill only talks about establishing one central Data Protection Authority.

Appointment of members

GDPR	PDP Bill
Member States to provide for each member of the supervisory authority to be appointed by in a transparent manner by (a) their Parliament; (b) their government; (c) their head of State; (d) an independent body.[89] Each member should have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.	Chairperson and the members of the Authority to be appointed by the Central Government on the recommendation of the Selection Committee.[90] Selection Committee to comprise of (a) Cabinet Secretary; (b) Secretary to the Government of India in the Law Ministry; and (c) Secretary to the Government of India in the External Affairs Ministry.

Under the GDPR, Member States are free to establish one or more supervisory authorities. Currently, the PDP Bill only talks about establishing one central Data Protection Authority.

87 Article 51(1)
88 Clause 41(1)
89 Article 53(1)
90 Clause 42(2)

Term of appointment

GDPR	PDP Bill
Minimum period of 4 years.[91] Eligibility of members to be reappointed is to be prescribed by law of the individual Member States.[92]	Maximum period of 5 years or till they attain the age of 65, whichever is earlier.[93] Members shall not be eligible for reappointment.

Under the GDPR, Member States are free to establish one or more supervisory authorities. Currently, the PDP Bill only talks about establishing one central Data Protection Authority.

Codes of Practice

GDPR	PDP Bill
Member States, the Supervisory Authority, the Board and the Commission shall encourage the drawing up of Code of Conduct intended to contribute to the proper application of the Regulations.[94] Associations and other authorities may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of the Regulation.[95] They shall prepare a draft code and submit it to the Supervisory Authority for approval.[96]	The Data Protection Authority shall issue Codes of Practice to promote good practices of data protection and facilitate compliance with the obligations under the Bill.[97] The Data Protection Authority may also approve,and issue codes of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government.[98]

Under the GDPR, Member States are free to establish one or more supervisory authorities. Currently, the PDP Bill only talks about establishing one central Data Protection Authority.

91 Article 54(1)(d)
92 Article 54(1)(e)
93 Clause 43(1)
94 Article 40(1)
95 Article 40 (2)
96 Article 40(5)
97 Clause 50(1)
98 Clause 50(2)

Complaint

GDPR

Data subject has the right to file a complaint with a supervisory authority. The authority has to inform the complainant about the progress and outcome of the complaint.[99]

PDP Bill

Data Principal has the right to file a complaint before the Data Protection Authority.[100]

Under the PDP Bill, the Data Protection Authority is not required to inform the data principal about the progress of the complaint.

Investigative Powers

GDPR

The Supervisory Authority has the following investigative powers[101]:

- To order the controller or the processor to provide any information it requires;
- To carry out investigations in the form of data protection audit
- To carry out a review of the certification issues pursuant to Article 42 (7)
- To notify the controller or the processor of an alleged infringement of the Regulation;
- to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

PDP Bill

The Data Protection Authority may conduct an inquiry where it has (a) reasonable grounds to believe that the activities of the data fiduciary or data processor is being conducted in a manner which is detrimental to the interests of the data principal, or (b) the data fiduciary or data processor has violated the provisions of the PDP Bill.

The Data Protection Authority shall appoint an inquiry officer to conduct an inquiry and submit a report to it.

Under the PDP Bill, the Data Protection Authority is not required to inform the data principal about the progress of the complaint.

99 Article 77(1)
100 Clause 53(1)
101 Article 58(1)

Powers of the Authority

GDPR

The Supervisory Authority has the following corrective powers:

- Issue a warning to a controller or a processor that the intended operations are likely to infringe the Regulations.
- Reprimand the controller or processor where an infringement has occurred.
- Order compliance with the request of the data subject and/or with the Regulations.
- Order the controller to communicate the data breach to the data subject
- Impose a temporary or definitive limitation on processing of data
- Order rectification or erasure of personal data
- Impose an administrative fine.
- Order the suspension of transfer of data to a third country.

PDP Bill

The Data Protection Authority can take the following steps:

- Issue a warning to the data fiduciary or data processor where the business is likely to infringe the Actl.
- Reprimand the data fiduciary or data processor if the business or activity has violated the Act.
- Require the data processor or data fiduciary to cease and desist from violating the provisions of the Act.
- Require the data processor or data fiduciary to modify the business activity to bring it in compliance with the Act.
- Temporarily suspend or discontinue business activity of the data fiduciary
- vary/suspend/cancel the registration granted by the Authority in case of a significant data fiduciary.
- Suspend or discontinue any cross border flow of personal data.

The powers of the Authority under the GDPR and the PDP Bill are substantially similar, however, under the PDP Bill, the Data Protection Authority has not been given an explicit power to order rectification or erasure of personal.

Right to approach courts

GDPR

The data subject has the right to approach the court where the supervisory authority does not handle a complaint or does not inform the data subject within 3 months on the progress or outcome of the complaint.[102]

PDP Bill

A person aggrieved with the decision of the Authority has the right to file an appeal before the Appellate Tribunal[103]. An appeal against the order of the Appellate Tribunal shall only lie before the Supreme Court

102 Article 78

103 Clause 72 (1)

11. Penalties and Compensation

Amount of penalty imposed

GDPR

It prescribes different ranges of penalties for contravention of different provisions.

It ranges from 10 000 000 EUR[104] to 20 000 000 EUR0[105], or in the case of an undertaking it ranges from 2% of the total worldwide turnover to 4% of the total worldwide turnover whichever is higher[106].

PDP Bill

It also prescribes different ranges of penalties for different provisions.

It ranges from Rs. 5 crore rupees or 2% of the total worldwide turnover of the preceding financial year[107], whichever is higher to Rs 15 crore or 4% of its total worldwide turnover of the preceding financial year, whichever is higher[108].

If any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter V of the Bill, such data fiduciary shall be liable to a penalty of Rs. 5000 for each day during which such default continues, subject to a maximum of Rs 10 lakh in case of significant data fiduciaries and Rs. 5 lakh in other cases.

Penalties significantly higher under the GDPR.

104 Article 83(4)
105 Article 83(5)
106 Article 83(6)
107 Clause 57(1)
108 Clause 57(2)

Failure to comply with the decision of the Authority

GDPR

Failure to comply with the decision of the supervisory authority is subject to a fine of up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

PDP Bill

If any data fiduciary or data processor fails to comply with any direction issued by the Data Protection Authority such data fiduciary or data processor shall be liable to a penalty which, in case of a data fiduciary may extend to Rs 20,000 rupees for each day during which such default continues, subject to a maximum of Rs. 2 crore, and in case of a data processor may extend to Rs. 5,000 for each day during which such default continues, subject to a maximum of Rs. 50 lakh.

Penalties significantly higher under the GDPR.

12. Offences

Re-identification and processing of personal data

GDPR	PDP Bill
Member States to lay down the rules on other penalties for infringements which are not subject to administrative fines. Such penalties shall be effective, proportionate and dissuasive.[109]	Any person who, knowingly or intentionally or recklessly— (a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or (b) re-identifies and processes such personal data as mentioned in clause (a) without the consent of such data fiduciary or data processor, then such person shall be punishable with imprisonment for a term not exceeding 3 years or shall be liable to a fine which may extend up to Rs 2 lakh or both.[110]

The GDPR does not harmonise the penalties- it is left to the Member States. However, the penalties have to be proportionate, effective and dissuasive. The nature of the penalties will be determined by the individual member states.

109 Article 84 (1)

110 Clause 82