ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

India

Status of Consent for Processing Personal Data

AUGUST 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTOR

Malavika Raghavan

Senior Fellow, Future of Privacy Forum

ACKNOWLEDGEMENTS

This Report benefitted contributions and editing support from Catherine Shen.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in India's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

To date, India has not enacted comprehensive data protection legislation.

Currently, the main data protection provisions in Indian law are found in the Information Technology Act 2000 ("**IT Act**")[1] as amended by the Information Technology (Amendment) Act 2008[2] and the subsidiary legislation to the IT Act,[3] including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("**IT Rules**").[4]

Certain sector-specific laws and regulations also contain provisions on personal data.

For example, the Aadhaar (Targeted Delivery of Financial and Other Subsidiaries, Benefits, and Services) Act 2016, as amended by the Aadhaar and Other Laws (Amendment) Bill 2019 permits financial institutions to use biometric information to verify individuals' identities when opening bank accounts. Additionally, the Credit Information Companies (Regulation) Act 2005, the Prevention of Money Laundering Act 2022, and the Payments and Settlements Act 2007, as well as various rules and regulations issued by the Reserve Bank of India, the Insurance Regulatory and Development Authority of India, and the Securities and Exchange Board of India all require regulated entities to keep identity information confidential and impose restrictions on when this information may be disclosed to third parties.[5]

In 2017, against the backdrop of the Supreme Court of India's landmark decision in *Justice KS Puttaswamy v. Union of India* ("***Puttaswamy***"),[6] which the found that privacy is a fundamental right protected by the Constitution of India, the Ministry of Electronics and Information Technology ("**MeitY**") established a Committee of Experts, led by retired Supreme Court Judge Justice BN Srikrishna to study issues relating to data protection in India, make recommendations for development of Indian law in this area, and ultimately, draft legislation. The Committee released a White Paper on a Data Protection Framework for India[7] for public comment in December 2017.

In July 2018, the Committee of Experts released draft data protection legislation, titled the Personal Data Protection Bill 2018, accompanied by a detailed report title "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians," explaining the Committee's rationale in drafting the legislation.[8] This draft Bill was subsequently approved by the Cabinet Ministry of India as the Personal Data Protection Bill 2019 ("**PDP Bill**")[9] and was tabled in the lower house of India's bicameral Parliament, the Lok Sabha, in December 2019. Between 2019 and 2021, the PDP Bill underwent review by a Joint Parliamentary Committee ("**JPC**"), which released a report ("**JPC Report**")[10] recommending changes to the draft PDP Bill in December 2021 – two years after the Bill was first tabled.

On August 3, 2022, India's Government withdrew the PDP Bill and announced that it was working on a new and comprehensive framework of data protection legislation, which it aimed to release for public

---

[1] Available at https://www.meity.gov.in/writereaddata/files/itbill2000.pdf
[2] Available at https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf
[3] Available at https://www.meity.gov.in/content/rules-information-technology-act-2000
[4] Available at https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf
[5] For a more detailed overview of relevant laws and regulations, see Dvara Research's responses to the Committee of Experts' Whitepaper on a Data Protection Framework for India (January 31, 2018), pages 23-35, available at https://www.dvara.com/research/blog/wp-content/uploads/2018/02/Response-to-White-Paper-Public-Consultation-Dvara-Research.pdf
[6] *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors* (2017) 10 SCC 1, available at https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
[7] Available at https://www.meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited
[8] Available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
[9] Available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
[10] Available at http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

comment in early 2023.[11] It remains unclear whether and to what extent the new legislation will adopt provisions for the former PDP Bill.

In any case, India is now several years away from adopting comprehensive data protection legislation as even if the new legislation is released within the next year, it would likely still be subject to public consultation and would have to be passed by both houses of India's Parliament and notified in the Official Gazette before it would take legal effect. Even if data protection legislation is enacted in future, it may not be fully implemented immediately after enactment; rather, implementation may take place in stages over a longer period of time.

2. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE IT ACT AND IT RULES

Section 43A of the amended IT Act requires private-sector entities – termed "**bodies corporate**"[12] – which possess, deal in, or handle "**sensitive personal information or data**" ("**SPDI**")[13] to implement and maintain reasonable security practices and procedures to protect the information from unauthorized access, damage, use, modification, or impairment. The IT Rules clarify a body corporate's obligations under Section 43A of the amended IT Act.

Notably, a body corporate or a person acting on its behalf must obtain written consent from a data subject before collecting that data subject's "SPDI."[14] The IT Rules do not provide any exceptions to this requirement.

Consent (termed "**permission**" in the IT Rules) is also the default requirement under the IT Rules for a body corporate or a person acting on its behalf to disclose SPDI to a third party.[15] However, the IT Rules provide exceptions to this requirement where:

- a contract between the body corporate and the information provider provides for such disclosure;
- disclosure is necessary for compliance with a legal obligation; or
- a government agency with a mandate to obtain information (including SPDI) for the purpose of identity verification or for prevention, detection, investigation, prosecution, and punishment of offenses (including cyber incidents) has sent a request in writing which clearly states the purpose for requesting the information.[16]

Lastly, consent is one of two legal bases (together with necessity for performance of a contract) under the IT Rules for transferring SPDI out of India.[17] This is subject to the rule that a body corporate or person acting on its behalf may only transfer such information to a country which ensures the same level of protection as that provided under the IT Rules.[18]

---

[11] Aditya Kalra and Aftab Ahmed, "India nixes privacy bill that alarmed big tech companies, works on new law" *Reuters* (5 August 2022), available at https://www.reuters.com/world/india/indian-government-withdraws-data-protection-bill-2022-08-03/

[12] Note that this term includes not only companies but also firms, sole proprietorships, and any association of individuals engaged in commercial or professional activities (IT Act, s 43A, Explanation (i)).

[13] The IT Rules define "**personal information**" as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person (IT Rules, r 2(i)) and "**sensitive personal data or information**" ("**SPDI**") as personal information which consists of information relating to: (i) a password; (ii) financial information; (iii) a physical, physiological, or mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to any of the foregoing as provided to a body corporate for providing a service; and (viii) any information received under any of the foregoing by a body corporate for processing, subject to exceptions (IT Rules, r 3).

[14] IT Rules, r 5(1).

[15] IT Rules, r 6(1).

[16] IT Rules, r 6(1).

[17] IT Rules, r 7.

[18] IT Rules, r 7.

The IT Rules also clarify when a body corporate or person acting on its behalf will be considered to have complied with the requirement to implement and maintain reasonable security practices and procedures under Section 43A of the IT Act.[19] Specifically, a body corporate which handles personal information, or a person acting on its behalf, must:

- provide a privacy policy, which must be made available to "providers of information" ("**information providers**") who have provided personal information under a lawful contract and must be published on the website of the body corporate or person acting on its behalf;[20]
- only collect SPDI which is necessary for a lawful purpose connected with a function or activity of the body corporate or person acting on its behalf;[21]
- take reasonable steps to inform data subjects of certain facts relating to collection of the "SPDI;"[22]
- retain SPDI for no longer than required;[23]
- use SPDI only for the purpose of collection;[24]
- provide information providers with access to personal information about them and ensure that such information is accurate;[25]
- provide information providers with the option not to provide their personal information before it is collected and to withdraw their consent to collection of personal information;[26]
- secure personal information;[27]
- provide a mechanism for addressing information providers' grievances;[28]
- obtain consent for disclosure of SPDI to any third party, subject to exceptions;[29] and
- only transfer SPDI out of India to countries which provide the same level of data protection as that provided under the IT Rules.[30]

Bodies corporate which are negligent in implementing and maintaining such practices and procedures and thereby cause wrongful loss or gain are liable to pay damages.

[19] IT Rules, r 8.
[20] IT Rules, r 4.
[21] IT Rules, r 5(2).
[22] IT Rules, r 5(3).
[23] IT Rules, r 5(4).
[24] IT Rules, r 5(5).
[25] IT Rules, r 5(6).
[26] IT Rules, r 5(7).
[27] IT Rules, r 5(8).
[28] IT Rules, r 5(9).
[29] IT Rules, r 6.
[30] IT Rules, r 7.

3. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE DRAFT PERSONAL DATA PROTECTION BILL ("PDP BILL") (WITHDRAWN)

Consent[31] would have been one of several legal bases for a "**data fiduciary**"[32] to process[33] the personal data of a "**data principal**"[34] under the PDP Bill.

Alternative legal bases to consent in the PDP Bill would have provided for processing of personal data without consent for performance of functions of State,[35] compliance with legal obligations,[36] necessity in emergency situations,[37] necessity in the employment context,[38] and necessity for a reasonable purpose.[39]

The PDP Bill also would have required data fiduciaries wishing to transfer "sensitive personal data" out of India to obtain the express consent of the data principal to such a transfer.[40]

4. CONDITIONS FOR CONSENT

4.1. Definition and forms of consent

a. IT Act and IT Rules

Neither the IT Act nor the IT Rules define "consent." The IT Rules require that consent to collection of SPDI must be obtained in writing through letter, facsimile, or email from the provider of such data.[41] These formal requirements do not appear to apply to consent for disclosure of SPDI to third parties. Note that for disclosure of such data to a third party, the IT Rules use the term "prior permission" rather than consent.[42]

b. PDP Bill (Withdrawn)

The PDP Bill would have required "consent"[43] to be:

- **free**, in the sense that the consent must not be procured through coercion, undue influence, fraud, misrepresentation, or mistake;[44]
- **informed**, having regard to whether at the time of collection, the data principal was provided with a notice containing the information in Section 7 of the PDP Bill;[45]

---

[31] PDP Bill, s 11(1).

[32] Note that a "**data fiduciary**" is defined as any person (including the State), a company, any juristic entity, or any individual who, alone or in conjunction with others, determines the purpose and means of processing of personal data (PDP Bill, 3(13)).

[33] Note that "**processing**" in relation to personal data is defined as an operation or set of operations performed on personal data, and may include operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure, or destruction (PDP Bill, s 3(31)).

[34] Note that a "**data principal**" is defined as the natural person to whom personal data relates (PDP Bill, s 3(14)).

[35] PDP Bill, s 12(a).

[36] PDP Bill, s 12(b).

[37] PDP Bill, s 12(d)-(f).

[38] PDP Bill, s 13.

[39] PDP Bill, s 14.

[40] PDP Bill, s 34(1). As to the scope of "sensitive personal data" under the PDP Bill, see "CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA" below.

[41] IT Rules, r 5(1).

[42] IT Rules, r 6(1).

[43] PDP Bill, s 3(10).

[44] PDP Bill, s 11(2)(a) read with Indian Contract Act, 1872, s 14.

[45] PDP Bill, s 11(2)(b).

- **specific**, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;[46]
- **clear**, having regard to whether the consent is indicated through an affirmative action that is meaningful in a given context;[47] and
- **capable of being withdrawn**, having regard to the ease of withdrawal compared with the ease with which consent can be given.[48]

Additionally, the PDP Bill would have held processing of "**sensitive personal data**" to a higher standard of consent (discussed in greater detail below).[49] Broadly, data fiduciaries seeking to process sensitive personal data would have been required to inform the data principal of any purpose or operation of processing that is likely to cause significant harm to the data principal.[50] Data fiduciaries also would not have been permitted to rely on inferred consent to process sensitive personal data.[51]

Lastly, the PDP Bill would have required consent for cross-border transfer of sensitive personal data to be "explicit."[52] The PDP Bill did not specify the conditions for explicit consent, though the wording of the relevant provision suggested that minimally, the data principal would have had to clearly and specifically consent to the transfer of his/her personal data out of India.

4.2. Withdrawal of consent

a. IT Rules

The IT Rules require that information providers should be given an option to refuse to provide their personal information prior to collection and to withdraw their consent to use of their personal information following collection.[53] Withdrawal of consent must take the form of a written notice, which must be sent to the body corporate.[54]

b. PDP Bill (Withdrawn)

One of the requirements for valid consent under the PDP Bill was that the consent had to be capable of being withdrawn.[55]

The PDP Bill also would have required a data fiduciary, at the time of data collection or as soon as reasonably practicable thereafter, to notify the data principal of his/her right to withdraw consent.[56] The notice would have had to explain the procedure for withdrawing consent[57] in a clear, concise, and easily comprehensible manner, in multiple languages where necessary and practicable.[58]

However, the PDP Bill also expressly stated that where the data principal withdraws consent to processing of personal data without any valid reason, then the data principal would have to bear all legal consequences for the effects of such withdrawal.[59] The JPC Report recommended removing the word "legal" from this provision to the effect that the data principal would bear all consequences (whether legal or otherwise) for withdrawing his/her consent without any valid reason.[60]

---

[46] PDP Bill, s 11(2)(c).
[47] PDP Bill, s 11(2)(d).
[48] PDP Bill, s 11(2)(e).
[49] PDP Bill, s 11(2).
[50] Note the definition of "**significant harm**" in PDP Bill, s 3(20)).
[51] PDP Bill, s 11(3)(b).
[52] PDP Bill, s 34(1).
[53] IT Rules, r 5(7).
[54] IT Rules, r 5(7).
[55] PDP Bill, s 11(2)(e).
[56] PDP Bill, s 7(1)(d).
[57] PDP Bill, s 7(1)(d).
[58] PDP Bill, s 7(2).
[59] PDP Bill, s 11(6).
[60] JPC Report, paragraph 2.56.

The PDP Bill also would have provided the data principal with a right to restrict or prevent the continuing disclosure of his/her personal data by a data fiduciary where such disclosure was originally made with the data principal's consent, but where such consent has since been withdrawn.[61]

4.3. Bundled consent

a. IT Rules

The IT Rules permit a body corporate to withhold provision of goods or services to a person who refuses to provide his/her personal information to the body corporate or to consent to collection and use of his/her personal information.[62]

b. PDP Bill (Withdrawn)

The PDP Bill would have expressly prohibited making provision or quality of any goods or services, or the performance of any contract, or the enjoyment of any legal right or claim, conditional on the consent to the processing of any personal data that is not necessary for that purpose.[63]

The JPC Report recommended expanding the scope of this provision so that the provision or quality of goods and services, the performance of a contract, or the enjoyment of any legal right or claim may not be denied based on any "exercise of choice."[64]

5. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

5.1. IT Rules

The IT Rules distinguish between "**personal information**" and "**sensitive personal data or information**" ("**SDPI**").

The IT Rules define "personal information" as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.[65]

The IT Rules define SPDI as a subset of personal information which has been provided to a body corporate in exchange for provision of a service[66] and received by a body corporate[67] and which consists of information relating to:

- passwords;[68]
- financial information, such as bank accounts, credit or debit cards, or other payment instrument details;[69]
- physical, physiological, and mental health conditions;[70]
- sexual orientation;[71]
- medical records and history;[72] or

---

[61] PBP Bill, s 20(1)(b).
[62] IT Rules, r 5(7).
[63] PDP Bill, s 11(4).
[64] JPC Report, paragraph 2.55.
[65] IT Rules, r 2(i).
[66] IT Rules, r 3(vii).
[67] IT Rules, r 3(viii).
[68] IT Rules, r 3(i). Note that a "**password**" is defined as a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information (IT Rules, r 2(h)).
[69] IT Rules, r 3(ii).
[70] IT Rules, r 3(iii).
[71] IT Rules, r 3(iv).
[72] IT Rules, r 3(v).

- biometric information.[73]

The IT Rules expressly exclude from the scope of SPDI any information that is freely available, accessible in public domain, or furnished under the Right to Information Act 2005 or any other law for the time being in force.

As discussed above, the IT Rules require written consent before SPDI can be collected,[74] and consent before SPDI can be disclosed to a third party (subject to exceptions).[75] The IT Rules also prescribe various security requirements for SPDI.

5.2. PDP Bill (Withdrawn)

a. Scope

The PDP Bill drew a distinction between "personal data" and "sensitive personal data."[76] The latter referred to a subset of personal data which may reveal, be related to, or constitute any of the following:

- financial data;[77]
- health data;[78]
- official identifiers;[79]
- a person's sex life[80] or sexual orientation;[81]
- biometric data;[82]
- genetic data;[83]
- transgender status;[84]

---

[73] IT Rules, r 3(vi). Note that "**biometrics**" are defined as technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes (IT Rules, r 2(b)).

[74] IT Rules, 5(1).

[75] IT Rules, rr 6(1) and 7.

[76] PDP Bill, s 3(36).

[77] PDP Bill, s 3(36)(i). Note that "**financial data**" is defined as any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history (PDP Bill, s 3(18)).

[78] PDP Bill, s 3(36)(ii). Note that "**health data**" is defined as data related to the state of physical or mental health of the data principal, including records regarding the past, present, or future state of the health of the data principal; data collected in the course of registration for, or provision of health services; and data associating the data principal to the provision of specific health services (PDP Bill, s 3(21)).

[79] PDP Bill, s 3(36)(iii). Note that an "**official identifier**" is defined as any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal (PDP Bill, s 3(26)).

[80] PDP Bill, s 3(36)(iv).

[81] PDP Bill, s 3(36)(v).

[82] PDP Bill, s 3(36)(vi). Note that "**biometric data**" is defined as facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioral characteristics of a data principal, which allow or confirm the unique identification of that natural person (PDP Bill, s 3(7)).

[83] PDP Bill, s 3(36)(vii). Note that "**genetic data**" is defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioral characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question (PDP Bill, s 3(19)).

[84] PDP Bill, s 3(36)(viii). Note that "**transgender status**" is defined as the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure (PDP Bill, s 3(36)(b)).

- intersex status;[85]
- caste or tribe;[86]
- religious or political belief or affiliation;[87] or
- any other data categorized as sensitive personal data by the Central Government under Section 15 of the PDP Bill.[88]

Section 15(1) of the PDP Bill would have empowered the Central Government, in consultation with the Data Protection Authority of India (once established) and relevant sectoral regulator(s), to notify new categories of sensitive personal data, having regard to:

- the risk of significant harm that may be caused to the data principal by the processing of such a category of personal data;[89]
- the expectation of confidentiality attached to such a category of personal data;[90]
- whether a significantly discernible class of data principals may suffer significant harm from the processing of such a category of personal data;[91] and
- the adequacy of protection afforded by ordinary provisions applicable to personal data.[92]

a. Requirements

A data fiduciary would only have been permitted to process sensitive personal data if the data fiduciary obtained consent from the data principal or satisfied the conditions for either a narrow list of alternative legal bases premised on necessity[93] or a "reasonable purpose" pursuant to Section 14 of the PDP Bill.[94]

The PDP Bill would have required a higher standard of consent for processing of sensitive personal data. Specifically, in addition to complying with the formal requirements for consent in Section 11(1) of the PDP Bill,[95] a data fiduciary seeking a data principal's consent for processing of his/her sensitive personal data would have had to obtain consent "explicitly" using clear terms without recourse to inference from conduct in a context[96] after

- informing the data principal of any purpose of, or operation in, processing which is likely to cause significant harm to him/her;[97] and
- giving him/her the choice of separately consenting to the purposes of, operations in, and use of different categories of sensitive personal data relevant to processing.[98]

The JPC Report found the phrase "in clear terms without recourse to inference from conduct in a context" ambiguous and recommended amending this provision so that when obtaining a data

---

85 PDP Bill, s 3(36)(ix). Note that "**intersex status**" is defined as the condition of a data principal who is: (i) a combination of female and male; (ii) neither wholly female nor wholly male; or (iii) neither female nor male (PDP Bill, s 3(36)(a)).
86 PDP Bill, s 3(36)(x).
87 PDP Bill, s 3(36)(xi).
88 PDP Bill, s 3(36)(xii).
89 PDP Bill, s 15(1)(a). Note that "**significant harm**" is defined as a harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm (PDP Bill, s 3(38)).
90 PDP Bill, s 15(1)(b).
91 PDP Bill, s 15(1)(c).
92 PDP Bill, s 15(1)(d).
93 See PDP Bill, s 12 and "Processing personal data without consent" below. Note that the legal basis of necessity for employment purposes in Section 13 of the PDP Bill is unavailable for processing of sensitive personal data.
94 See "COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT" below.
95 i.e., that consent must be free, informed, specific, clear, and capable of being withdrawn.
96 PDP Bill, s 11(3)(b).
97 PDP Bill, s 11(3)(a). Note the definition of "**significant harm**" in PDP Bill, s 3(38).
98 PDP Bill, s 11(3)(c).

principal's consent, the party seeking consent should specify "the conduct and context explicitly without circumvention of law and without any kind of implicit inferences."[99]

In addition to the above requirements, the PDP Bill would have empowered the Data Protection Authority of India (once established) to make regulations to specify additional safeguards or restrictions for collection of sensitive personal data.[100]

5.3. Children

a. IT Rules

The IT Rules do not make specific provisions for children's personal information.

b. PDP Bill (Withdrawn)

Under the PDP Bill, the personal data of children would not have automatically qualified as sensitive personal data, unless the data in question falls within any of the categories outlined in Section 3(36) of the PDP Bill.

However, the PDP Bill proposed specific provisions for processing of the personal data of a "child" (defined as a person who has not yet reached the age of 18).[101] Before processing a child's personal data, the data fiduciary would have had to verify the child's age and obtain the consent of the child's parent or guardian.[102] The PDP Bill provided that the method for verifying the child's age would be specified in regulations,[103] taking into consideration:

- the volume of personal data processed;[104]
- the proportion of data principals in that data who are likely to be children;[105]
- the possibility of harm to a child arising out of the processing of personal data;[106] and
- any other prescribed factors. [107]

If enacted, the PDP Bill would have empowered the Data Protection Authority of India (once established) to issue regulations to classify any data fiduciary who operated commercial websites directed at children[108] or processed large volumes of personal data of children as a "guardian data fiduciary."[109] A guardian data fiduciary would have been barred from profiling, tracking, or behaviorally monitoring children and from undertaking any other processing of personal data that may cause significant harm to a child.[110]

The JPC Report raised concerns that the concept of a "guardian data fiduciary" was undefined in the 2019 draft of the PDP Bill, that there appeared to be no advantage to establishing a new category of data fiduciary, and that this may have led to circumvention and dilution of law.[111] The JPC therefore recommended removing the concept from the PDP Bill entirely.

5.4. Cookies, Internet of Things, online tracking

Neither the IT Rules nor the PDP Bill (withdrawn) make specific provisions for cookies, the Internet of Things, or online tracking (except in the context of children's data – see above).

---

[99] JPC Report, paragraph 2.54.
[100] PDP Bill, s 15(2).
[101] PDP Bill, s 3(8).
[102] PDP Bill, s 16(2).
[103] PDP Bill, ss 16(2) and 16(3).
[104] PDP Bill, s 16(3)(a).
[105] PDP Bill, s 16(3)(b).
[106] PDP Bill, s 16(3)(c).
[107] PDP Bill, s 16(3)(d).
[108] PDP Bill, s 16(4)(a).
[109] PDP Bill, s 16(4)(b).
[110] PDP Bill, s 16(5). Note the definition of "**significant harm**" in PDP Bill, s 3(38).
[111] JPC Report, paragraph 2.75.

5.5. Direct marketing

Neither the IT Rules nor the PDP Bill (withdrawn) make specific provisions for direct marketing.

5.6. Biometric data

Both the IT Rules[112] and the PDP Bill (withdrawn)[113] classify biometric data as sensitive personal data.

5.7. Genetic data

The IT Rules do not expressly classify genetic data as SPDI, though note that biometric information is categorized as SPDI,[114] and the IT Rules' definition of "biometrics" includes DNA when used for authentication purposes.[115]

By contrast, the PDP Bill (withdrawn) expressly classified genetic data as sensitive personal data.[116]

5.8. Financial information

Both the IT Rules[117] and the PDP Bill (withdrawn)[118] classify financial information as sensitive personal data.

5.9. Statistics and research

The IT Rules do not provide for collection, use, or disclosure of personal information for statistical or research purposes.

By contrast, the PDP Bill (withdrawn) would have empowered the Data Protection Authority of India (once established) to issue regulations to:

- exempt processing of personal data from the application of any provisions of the PDP Bill, where such processing is necessary for a specified research, archiving, or statistical purpose;[119] and
- specify a code of practice to promote good data protection practice and facilitate compliance with the PDP Bill in relation to processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes.[120]

5.10. Pseudonymized data

Neither the IT Rules nor the PDP Bill (withdrawn) specifically provide for pseudonymized data.

---

[112] IT Rules, r 3(vi). Note that "**biometrics**" are defined as technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes (IT Rules, r 2(b)).

[113] PDP Bill, s 3(36)(vi). Note that "**biometric data**" is defined as facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioral characteristics of a data principal, which allow or confirm the unique identification of that natural person (PDP Bill, s 3(7)).

[114] IT Rules, r 3(iv).

[115] IT Rules, r 2(b).

[116] PDP Bill, s 3(36)(vii). Note that "**genetic data**" is defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioral characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question (PDP Bill, s 3(19)).

[117] IT Rules, r 3(ii).

[118] PDP Bill, s 3(36)(i). Note that "**financial data**" is defined as any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history (PDP Bill, s 3(18)).

[119] PDP Bill, s 38.

[120] PDP Bill, ss 50(1) and 50(6)(r).

Insofar as pseudonymized personal information is capable of identifying a natural person when combined with other available information, then such information would fall within the IT Rules' definition of "personal information."[121]

5.11. Location data

Neither the IT Rules nor the PDP Bill specifically provide for location data.

6. CONSENT FOR CROSS-BORDER DATA TRANSFERS

6.1. IT Rules

The IT Rules provide for cross-border transfer of SPDI but do not specifically provide for cross-border transfer of personal data or information that falls outside of this definition.

The IT Rules permit a body corporate or any person acting on its behalf to transfer SPDI out of India, provided that:

- the recipient is located in a jurisdiction that ensures "the same level of data protection that is adhered to by the body corporate as provided for under the IT Rules;" and
- either:
  - the information provider consents to the transfer; or
  - the transfer is necessary for performance of a lawful contract between the information provider and the body corporate or person acting on its behalf.[122]

6.2. PDP Bill (Withdrawn)

The PDP Bill would have required a data fiduciary to obtain a data principal's explicit consent before transferring the data fiduciary's sensitive personal data outside of India,[123] and comply with other relevant requirements for authorization of the transfer by the Data Protection Authority of India and/or the Central Government, as appropriate.[124]

The PDP Bill also would have required any data fiduciary that intended to transfer personal data across borders, to notify the data principal of this intention whenever the data fiduciary collected personal data from the data principal.[125]

Further, pursuant to the data fiduciary's obligation to maintain transparency in processing personal data (see below), the data fiduciary would be required to provide information regarding cross-border transfers of personal data that the data fiduciary generally carries out in the form and manner prescribed by regulation.[126]

7. TRANSPARENCY AND NOTICE

7.1. IT Rules

Under the IT Rules, a body corporate or a person acting on its behalf must take such steps as are reasonable in the circumstances to ensure that a person from whom information is collected has knowledge of the following:

---

[121] IT Rules, s 2(l).
[122] IT Rules, r 7.
[123] PDP Bill, s 34(1).
[124] See PDP Bill, ss 34(1)(a), 34(1)(b), and 34(1)(c).
[125] PDP Bill, s 7(1)(h).
[126] PDP Bill, s 23(1)(f).

- the fact that the information is being collected;[127]
- the purpose for which the information is being collected;[128]
- the intended recipients of the information;[129] and
- the name and address of —
  - the agency that is collecting the information;[130] and
  - the agency that will retain the information.[131]

7.2. PDP Bill (Withdrawn)

The PDP Bill would have required that consent for processing of personal data must be Informed.[132] To satisfy this condition, the data fiduciary would have had to provide the following information to the data principal, at the time of data collection or as soon as reasonably practicable thereafter:

- the purposes for which the personal data is to be processed;[133]
- the nature and categories of personal data that are being collected;[134]
- the identity and contact details of the data fiduciary, and the contact details of the data protection officer, if applicable;[135]
- the right of the data principal to withdraw consent, and the procedure for withdrawing consent;[136]
- if the personal data is not collected from the data principal, the source from which the personal data is collected;[137]
- the individuals or entities – including other data fiduciaries or data processors – with whom such personal data may be shared, if applicable;[138]
- information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;[139]
- the period for which the personal data shall be retained, or where such period is not known, the criteria for determining such a period;[140]
- the existence of and procedure for the exercise of the data principal's rights under Chapter V of the PDP Bill, and any related contact details;[141]
- the procedure for grievance redressal;[142]
- the existence of a right to file complaints to the Data Protection Authority of India;[143]
- where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under Section 29(5) of the PDP Bill;[144] and

---

127 IT Rules, r 5(3)(a).
128 IT Rules, r 5(3)(b).
129 IT Rules, r 5(3)(c).
130 IT Rules, r 5(3)(d)(i).
131 IT Rules, r 5(3)(d)(ii).
132 PDP Bill, s 11(2)(b).
133 PDP Bill, s 7(1)(a).
134 PDP Bill, s 7(1)(b).
135 PDP Bill, s 7(1)(c).
136 PDP Bill, s 7(1)(d).
137 PDP Bill, s 7(1)(f).
138 PDP Bill, s 7(1)(g).
139 PDP Bill, s 7(1)(h).
140 PDP Bill, s 7(1)(i).
141 PDP Bill, s 7(1)(j).
142 PDP Bill, s 7(1)(k).
143 PDP Bill, s 7(1)(l).
144 PDP Bill, s 7(1)(m).

- any other information as may be specified by regulation.[145]

The data fiduciary would have been required to present this in a manner that is clear, concise, and easily comprehensible to a reasonable person, in multiple languages where necessary and practicable.[146]

A data fiduciary would also have been required to take necessary steps to maintain transparency in processing personal data and make the following information available in such form and manner as may be specified by regulations:

- the categories of personal data generally collected and the manner of such collection;[147]
- the purposes for which personal data is generally processed;[148]
- any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;[149]
- the existence of and procedure for the exercise of the data principal's rights under Chapter V of the PDP Bill, and any related contact details; [150]
- the existence of a right to file complaints to the Data Protection Authority of India; [151]
- where applicable,
  - any rating in the form of a data trust score that may be assigned to the data fiduciary under Section 29(5) of the PDP Bill;[152]
  - information regarding cross-border transfers of personal data that the data fiduciary generally carries out;[153] and
- any other information as may be specified by regulations.[154]

8. MANAGEMENT OF CONSENT

The PDP Bill caused confusion by referring to the novel concept of a "consent manager" in several provisions. Specifically:

- Sections 23(3) and 23(4) of the PDP Bill state that a data principal may, respectively, give or withdraw consent via a consent manager, and that if a data principal does so, then the giving or withdrawal of consent shall be deemed to have been communicated directly by the data principal.
- Section 23(5) of the PDP Bill requires a consent manager to register with the Data Protection Authority of India (once established).
- Lastly, Section 93(1)(h) of the PDP Bill states that the Central Government may by notification make rules as to the manner and the technical, operation, financial and other conditions for registration of the consent manager and its compliance with Section 23(5).

It was unclear from the PDP Bill what this term refers to, though note that the Explanation to Section 23(5) of the PDP Bill stated that a "consent manager" is a data fiduciary which enables a data principal to obtain, withdraw, review, and manage consent through an accessible, transparent, and interoperable platform.

---

145 PDP Bill, s 7(1)(n).
146 PDP Bill, s 7(2).
147 PDP Bill, s 23(1)(a).
148 PDP Bill, s 23(1)(b).
149 PDP Bill, s 23(1)(c).
150 PDP Bill, s 23(1)(d).
151 PDP Bill, s 23(1)(e).
152 PDP Bill, s 23(1)(f).
153 PDP Bill, s 23(1)(g).
154 PDP Bill, s 23(1)(h).

However, there had been speculation that the term "consent manager" in the PDP Bill refers to Data Empowerment and Protection Architecture ("**DEPA**")[155] – a proposal by NITI Aayog (a think tank within the Government of India) to establish a private institution to act as a middleman between users and providers of information to facilitate data flows from entities that currently hold Indians' personal data to other data businesses that might want to use this data, with the permission of the data principal. NITI Aayog hopes to deploy DEPA first in the financial sector and then tailor it to apply flexibly in other sectors, including health and telecoms.

It remains unclear whether these proposals will be adopted in future data protection legislation in India.

However, as to what form this "consent manager" may eventually take, an Indian technology group called iSpirit has proposed incorporating consent as a fourth "layer" to IndiaStack – a set of open APIs intended to allow governments, businesses, start-ups, and developers to utilize digital infrastructure to enable presence-less, paperless, and cashless service delivery[156] which currently consists of three "layers": (1) "presence-less" (a universal biometric digital identity allowing Indians to participate in any service from anywhere in the country), (2) "paperless" (digital records attached to an individual's digital identity), and (3) "cashless" (single interface to all the country's bank accounts and wallets to democratize payments).[157]

iSpirit's proposed solution focuses on privacy self-management by the user through a smartphone interface and seeks to digitize and facilitate the giving of consent for data sharing with service providers. A back-end system would then share the subject's data directly between providers, based on the data subject's choices.

9. SANCTIONS AND ENFORCEMENT

9.1. IT Act

Section 72 of the IT Act prescribes a penalty for "breach of confidentiality and privacy." Under this provision, it is an offense for a person who has secured access to information pursuant to powers granted by the IT Act to disclose that information to a third party without "the consent of the person concerned."

Section 72A of the amended IT Act also prescribes a punishment for any person who discloses personal information about another person without that person's consent with intent to cause, or knowing that disclosure would be likely to cause wrongful loss or wrongful gain.

Section 43A of the amended IT Act provides that a body corporate which:

- possesses, deals in, or handles any SPDI in a computer resource which it owns, and
- is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person,

is liable to pay damages in compensation to the person affected.[158]

9.2. PDP Bill (Withdrawn)

a. Fines

If the PDP Bill had been enacted, a data fiduciary who processed:

- personal data in violation of any of the requirements in Chapters II and III of the PDP Bill,[159] including the requirement to obtain valid consent if another legal basis is unavailable; or

---

[155] NITI Aayog, "Data Empowerment and Protection Architecture Executive Summary" (August 2020), available at https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Executive-Summary.pdf

[156] See https://www.indiastack.org/

[157] See https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/

[158] Note that s 46 of the IT Act empowers adjudicating officers to adjudicate claims up to 5 crore (fifty million) rupees. For claims exceeding that amount, jurisdiction is with the competent court.

[159] PDP Bill, s 57(2)(a).

- the personal data of children in violation of any of the requirements of Section 16 of the PDP Bill,[160] including the requirement to verify the child's age and seek consent from the child's parent or guardian

would have faced a fine of up to INR fifteen crore (150,000,000) or 4% of the data fiduciary's total worldwide turnover for the preceding financial year (whichever is higher).

b. Liability to pay compensation

Additionally, a data principal who has suffered harm as a result of a data fiduciary or data processor's breach of any of the provisions of the PDP Bill would have had a right to seek compensation from the data fiduciary or data processor.[161]

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

If enacted, the PDP Bill would have provided a legal basis for processing of a data principal's personal data without the data principal's consent if such processing is necessary for a "reasonable purpose" specified by regulations,[162] after taking into consideration:

- the interest of the data fiduciary in processing for that purpose;[163]
- whether the data fiduciary could reasonably be expected to obtain the data principal's consent;[164]
- any public interest in processing for that purpose;[165]
- the effect of processing on the data principal's rights;[166] and
- the reasonable expectation of the data principal.[167]

The PDP Bill provided that the Data Protection Authority of India (once established) would specify "reasonable purposes" by regulation.[168] In this regard, Section 14(2) of the PDP Bill listed the following as possible examples of "reasonable purposes:"

- prevention and detection of any unlawful activity including fraud;[169]
- whistle blowing;[170]
- mergers and acquisitions;[171]
- network and information security;[172]
- credit scoring;[173]
- recovery of debt;[174]

---

[160] PDP Bill, s 57(2)(b).
[161] PDP Bill, s 64(1).
[162] PDP Bill, s 14(1).
[163] PDP Bill, s 14(1)(a).
[164] PDP Bill, s 14(1)(b).
[165] PDP Bill, s 14(1)(c).
[166] PDP Bill, s 14(1)(d).
[167] PDP Bill, s 14(1)(e).
[168] PDP Bill, s 14(1).
[169] PDP Bill, s 14(2)(a).
[170] PDP Bill, s 14(2)(b).
[171] PDP Bill, s 14(2)(c). Note that the JPC Report at paragraph 2.65 recommends broadening the scope of this provision to include "any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws."
[172] PDP Bill, s 14(2)(d).
[173] PDP Bill, s 14(2)(e).
[174] PDP Bill, s 14(2)(f).

- processing of publicly available personal data;[175] and
- the operation of search engines.[176]

Thereafter, the authority would also have been required to:

- issue regulations laying down appropriate safeguards to ensure the protection of the rights of data principals;[177] and
- determine whether notice will be required in relation to the reasonable purpose, having regard to whether such notice would substantially prejudice the relevant reasonable purpose.[178]

The JPC Report makes several recommendations regarding the balancing test under Section 14(1) of the PDP Bill:[179]

- adding the word "legitimate" to PDP Bill, s 14(1)(a) so that when determining reasonable purposes for which personal data may be processed without the data principal's consent, the regulator would have had to take into consideration the legitimate interests of the data fiduciary in processing for that purpose;
- adding reference to practicability to PDP Bill, s 14(1)(b), so that the regulator would have had to take into consideration not only whether the data fiduciary could reasonably be expected to obtain the data principal's consent but also whether obtaining consent would be practicable;
- refining the scope of "the effect of processing on the data principal's rights" so that the regulator would have had to consider the degree of any adverse effect from processing on the rights of the data principal, rather than simply considering the effect of such processing on the data principal's rights.

Apart from the above, the PDP Bill would not have expressly required data fiduciaries to conduct a data protection impact assessment for most forms of processing.

11. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

11.1. IT Rules

a. Collecting SPDI

Consent is the sole legal basis for collection of SPDI under the IT Rules[180] and is the main legal basis for disclosure of SPDI to a third party.[181]

b. Disclosing SPDI to a third party

The IT Rules recognize alternative legal bases for disclosing SPDI to a third party. A body corporate may also disclose such information to a third party if:

- a contract between the information provider and the body corporate provides for such disclosure, or
- such disclosure is necessary for compliance with a legal obligation.[182]

Additionally, the IT Rules permit disclosure of SPDI to a government agency which:

---

[175] PDP Bill, s 14(2)(g).
[176] PDP Bill, s 14(2)(g).
[177] PDP Bill, s 14(3)(a).
[178] PDP Bill, s 14(3)(b).
[179] JPC Report, paragraph 2.65.
[180] IT Rules, r 5(1).
[181] IT Rules, r 6(!).
[182] IT Rules, r 6(1).

- has a legal mandate to obtain such information for:
  - the purpose of identity verification; or
  - prevention, detection, investigation including cyber incidents, prosecution, and punishment of offenses; and
- has sent a request to the body corporate which possesses the SPDI clearly stating the purpose for requesting the information.[183]

c. Transferring SPDI across borders

The IT Rules permit transfer of SPDI to a recipient outside of India without the consent of the information provider where the cross-border transfer is necessary for performance of a lawful contract between the body corporate or any person on its behalf and the information provider.[184]

This is subject to the requirement that the recipient must be located in a country which ensures the same level of data protection as that to which the body corporate or person acting on its behalf is bound to provide under the IT Rules.[185]

11.2. PDP Bill (Withdrawn)

a. Processing personal data without consent

The PDP Bill would have provided for several legal bases beyond consent for processing personal data.

i. Necessity for compliance with legal obligations

The PDP Bill would have permitted a data fiduciary to process personal data of a data principal without the data principal's consent if such processing were necessary:

- for performance of any function of State authorized by law for:
  - the provision of any service or benefit to the data principal from the State;[186] or
  - the issuance of any certification, license, or permit for any action or activity of the data principal by the State;[187]
- under any law for the time being in force made by Parliament or any State Legislature;[188] or
- for compliance with any order or judgement of any Court or Tribunal in India.[189]

ii. Necessity in an emergency

The PDP Bill would have permitted a data fiduciary to process personal data of a data principal without the data principal's consent if such processing were necessary 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;[190]
- 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;[191] or
- undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.[192]

---

[183] IT Rules, r 6(1).
[184] IT Rules, r 7.
[185] IT Rules, r 7.
[186] PDP Bill, s 12(a)(i).
[187] PDP Bill, s 12(a)(ii).
[188] PDP Bill, s 12(b).
[189] PDP Bill, s 12(c).
[190] PDP Bill, s 12(d).
[191] PDP Bill, s 12(e).
[192] PDP Bill, s 12(f).

iii. Necessity in employment context

The PDP Bill would have permitted a data fiduciary to process personal data (but not sensitive personal data) of a data principal where the data principal is a prospective or current employee of a data fiduciary, and:

- obtaining consent would either:
  - be inappropriate having regard to the employment relationship, or
  - involve disproportionate effort on the part of the data fiduciary due to the nature of processing,[193] and
- processing were necessary for:
  - recruitment of the data principal or termination of the data principal's employment by the data fiduciary;[194]
  - verifying the data principal's attendance;[195] or
  - any other activity relating to the assessment of the data principal's performance.[196]

The JPC Report recommended introducing an alternative to the necessity standard in Section 13(1) of the PDP Bill, so that an employer would be permitted to process the personal data of an employee without the employee's consent if the processing is either necessary for any of the foregoing purposes or if the employee would reasonably expect that his/her personal data would be processed for any of these purposes.[197]

b. Exemptions from the PDP Bill

Chapter VIII of the PDP Bill would have provided explicit exemptions to the PDP Bill's consent requirements.

i. General exemptions

The PDP Bill's consent requirements, among others, would not have applied where:

- personal data were processed in the interests of prevention, detection, investigation, and prosecution of any offense or of any other contravention of any law for the time being in force;[198]
- disclosure of personal data were necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding;[199]
- processing of personal data by any court or tribunal in India were necessary for the exercise of any judicial function;[200]
- personal data were processed by a natural person for any personal or domestic purpose, except where such processing involved disclosure to the public, or were undertaken in connection with any professional or commercial activity;[201]

[193] PDP Bill, s 13(2).
[194] PDP Bill, s 13(1)(a).
[195] PDP Bill, s 13(1)(b).
[196] PDP Bill, s 13(1)(c).
[197] JPC Report, paragraph 2.61.
[198] PDP Bill, s 36(a).
[199] PDP Bill, s 36(b).
[200] PDP Bill, s 36(c).
[201] PDP Bill, s 36(d).

- processing of personal data were necessary for or relevant to a journalistic purpose, by any person and were in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organization.[202]

ii. Central Government powers to exempt

Additionally, the PDP Bill would have granted the Central Government powers to exempt certain parties from obligations under the PDP Bill, including the obligation to seek consent.

Firstly, the Central Government would have been empowered to order that any/all of the provisions of the PDP Bill shall not apply to a government agency in respect of data processing if the Central Government is satisfied that such order is necessary or expedient:

- in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order;[203] or
- for preventing incitement to the commission of any cognizable offense relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order.[204]

Secondly, the Central Government would have been empowered to issue a notification exempting from the application of the PDP Bill the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.[205]

iii. Data Protection Authority's power to exempt for research, archiving, or statistical purposes

Lastly, the PDP Bill would have empowered the Data Protection Authority of India (once established) to issue a notification to exempt the processing of personal data research, archiving, or statistical purposes from any of the provisions of the PDP Bill where the Authority were satisfied that:

- compliance with the provisions of the PDP Bill would disproportionately divert resources from such a purpose;[206]
- the purposes of processing could not be achieved if the personal data is anonymized;[207]
- the data fiduciary had carried out de-identification in accordance with the code of practice specified under Section 50 of the PDP Bill, and the purpose of processing can be achieved if the personal data is in de-identified form;[208]
- the personal data would not be used to take any decision specific to or action directed to the data principal;[209] and
- the personal data would not be processed in the manner that gives rise to a risk of significant harm to the data principal.[210]

Note also that the Authority would also have been empowered to specify a code of practice to promote good data protection practice and facilitate compliance with the PDP Bill in relation to processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes.[211]

---

[202] PDP Bill, s 36(e). Note that a "**journalistic purpose**" is defined as any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views, or documentaries regarding: (i) news, recent or current events; or (ii) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in (PDP Bill, s 3(24)).
[203] PDP Bill, s 35(i).
[204] PDP Bill, s 35(ii).
[205] PDP Bill, s 37.
[206] PDP Bill, s 38(a).
[207] PDP Bill, s 38(b).
[208] PDP Bill, s 38(c).
[209] PDP Bill, s 38(d).
[210] PDP Bill, s 38(e).
[211] PDP Bill, ss 50(1) and 50(6)(r).

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG