client alert

August 03, 2023

cyril amarchand mangaldas
ahead of the curve

Of Consent and Lawful Uses: Where the Rubber meets the Road

While the concept of consent, in consonance with the current consent based regime under the Information Technology Act, 2000 (**"IT Act"**)[1] as well as the constitutional primacy of consent and autonomy under various court decisions dealing with the right to information privacy has remained firmly entrenched as the primary basis for collection and processing of personal data under the various drafts of general personal data protection legislation in India over the years,[2] the newly notified Digital Personal Data Protection Act, 2023 ("**Act**")[3] also provides for "legitimate use" as key additional basis available to Data Fiduciaries[4] for collection and processing of personal data[5].

As a part of our series on the Act, we now examine how the Act deals with consent as well as legitimate use, as against the draft Digital Personal Data Protection Bill, 2022 (**"Draft"**)[6] and some global frameworks.

Notice and Consent

The Act continues to require that consent be free, specific, informed, unconditional, express and signified through an affirmative act.[7]

Under the Act, this notice must be given each time consent is sought,[8] potentially increasing the size of the tsunami of notices (and attendant fatigue) that Indians will soon be subject to.

The Act also continues to require that fresh notice be provided where processing has been consented to previously.[9] In India, where consent was only required for processing a narrowly defined set of 'sensitive personal data or information' under the IT Act,[10] Data Fiduciaries will

1 The Information Technology Act, 2000 ("**IT Act**") read with Rule 5, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**"SPDI Rules"**), available here.
2 The Draft, available here, the Report of the Joint Committee on the Personal Data Protection Act, 2019 (**"2021 Act"**), available here, the Personal Data Protection Act, 2019 (**"2019 Act"**), available here and the Personal Data Protection Act, 2018, available here.
3 The Digital Personal Data Protection Act, 2023 ("**Act**"), available here.
4 Section 2(i), Act: "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
5 Section 2(t), Act: "personal data" means any data about an individual who is identifiable by or in relation to such data.
6 The Digital Personal Data Protection Bill, 2022 ("**Draft**"), here.
7 Section 6(1), Act.
8 Section 5(1), Act.
9 Section 5(2), Act
10 IT Act read with Rule 5, SPDI Rules.

have to examine their previous consents carefully, provide fresh notices, and (potentially) take fresh consents after the Act officially comes into force. It may therefore be useful to clarify the position around legacy personal data that has been processed without specific consent, where the law did not require the same. Data Fiduciaries can continue to process personal data for whose processing consent was collected prior to enactment of the Act[11], by providing notice in prescribed form[12], and in a move that will be welcomed by businesses, the Act clarifies that Data Fiduciaries may continue to process personal data until the Data Principal[13] withdraws consent[14].

Importantly, in a position that is currently more liberal than much of the other legislations around the world,[15] it currently allows consolidated consent to be taken by giving notice (clear, comprehensible, available in multiple languages, *listing* the purposes for which data may be processed, the manner in which a Data Principal may exercise her rights and the manner in which a complaint may be made to the Board) in a manner that may be specified.

Unlike the Draft, the Act no longer expressly requires that those notices list purposes in itemized form, and rather requires that notice be in a manner that will be prescribed.[16]

While this leaves open the possibility of a more onerous requirement for granular consents (i.e., separate consents for each purpose)[17], the Act also appears to address the concern of "all or nothing" bundled consents in a different manner.

Interestingly, in a change that appears intended to codify purpose limitation and avoid bundling, the Act includes:

a. new language, which deems that any consent granted will only be limited to "such personal data as is necessary for the specified purpose"[18]; and

b. an illustration, which deems that even where the use of two independent sets of data ("personal data" and "mobile phone contact list") are separately listed and consented to, consent will be deemed to be limited to the former, as the latter is not "necessary".[19]

While the former is welcome, the latter is problematic for two reasons:

a. Firstly, while the section clearly enables Data Fiduciaries to indicate the necessity of a purpose and obtain consent for it, the illustration seems to require justifying "necessity" independently and narrows the section; and

b. Secondly, the illustration drifts into the realm of anticipation and business judgement, which is always a bad idea in the technology space. For instance, a telehealth provider may use address book information to enable automatic population of emergency/caregiver contact information for older patients, or enable loyalty, marketing or delivery programs for medicine to friends and family in exchange for benefits. By tritely assuming that this information is not necessary, the illustration may be unnecessarily restrictive.

11 Section 5(2), Act.
12 Sections 5(2) and 40(2)(b), Act.
13 Section 2(j), Act: "Data Principal" means the individual to whom the personal data relates and where such individual is—
   i a child, includes the parents or lawful guardian of such a child; and
   ii a person with disability, includes her lawful guardian, acting on her behalf.
14 Section 5(2)(b), Act.
15 Article 7, General Data Protection Regulation (**"GDPR"**), available here.
16 Section 5(2), Act.
17 Section 6(2), Act.
18 Section 6(1), Act.
19 Illustration to Section 6(1), Act.

The Act mirrors the position on withdrawal of consent as was specified in the Draft.[20] Data Principals have a right to withdraw consent for processing of data as easily as the manner for consent. However, such withdrawal would not affect the lawfulness of processing done prior to the withdrawal.[21] Upon withdrawal, the Data Fiduciary is required to cease processing of such personal data "within a reasonable time", unless such processing is authorised under law.[22] The consequences of such withdrawal would be borne by the Data Principal.[23] In another move to strengthen consent, the Act extends the obligation of erasure of data upon withdrawal of consent to both the Data Fiduciary, and entities processing data on its behalf.[24]

Legitimate Use

The introduction of "deemed" consent, potentially from Singapore's Personal Data Protection Act, 2012 (**"PDPA"**)[25], in place of "reasonable purpose" exceptions under the Draft was the *locus* of much debate. The Act replaces this concept with a more palatable concept of "legitimate use" and also ushers in significant changes, some of which may prove problematic:

a. While processing information provided "voluntarily" is recognized as a legitimate use and basis for processing, it will only operate for specified purposes, and only continue till such time as it is not withdrawn[26]. Problematically, the requirement of a "reasonable expectation"[27] of processing is gone, and consent seems to be deemed for all voluntary submission,[28] which may significantly narrow cases where express consent is taken.

b. A broadly worded "legitimate use" exception for processing by the government (or its instrumentalities) for granting benefits, subsidy, license, service, certificate or permit, (as clarified by an interesting illustration)[29], subject to compliance with standards for such processing being in accordance with central government policy or law, has been included.[30] The inclusion of 'services' means that this legitimate use is an extensive basis for processing. Further, compliance with central government policy will make standards like the National Data Governance Policy and potentially, the National Digital Health Scheme of primary importance. Similarly, the legitimate use exception has been extended to processing for performance of function under any law, in the interest of sovereignty, integrity and security of the State[31] and disclosure of information by any person for fulfilling an obligation under law.[32]

c. Legitimate use is also recognized for processing for compliance with any judgment in India and has been extended to judgments "relating to" claims of a civil or contractual nature under laws in force outside India.[33] It will be interesting to see how contempt orders of foreign courts (in civil disputes) are treated with this language.

d. Legitimate use for the purposes of employment continues to be presumed, but with significant modifications. While processing for "employment purposes" has been retained[34], the focus of this legitimate use seems to now be squarely on safeguarding the employer from loss or liability or providing a benefit sought by the employee.

20 Sections 6(4), 6(5), Act and 6(4), Draft.
21 Section 6(5), Act.
22 Section 6(6), Act.
23 Section 6(5), Act.
24 Section 8(7), Act
25 Section 15, PDPA, available here.
26 Section 7(a), Act.
27 Section 8(9)(c), Draft.
28 Section 7(a), Act.
29 Illustration to Section 7(b), Act.
30 Section 7(b), Act.
31 Section 7(c), Act.
32 Section 7(d), Act.
33 Section 7(e), Act.
34 Section 7(i), Act.

Given the removal of clear inclusions like recruitment and attendance,[35] employers may be well advised to rely on consent for much of their processing.

A somewhat problematic change in the Act may be the removal of deemed consent exceptions for what were erroneously called public interest purposes[36] but translated into "reasonable purpose" processing in much of the world.

Entirely omitted are key reasonable purpose exceptions like prevention of fraud, network and information security, and operation of search engines.

While the exclusion of all personal data which has been made public by the Data Principal (or by operation of law) from the ambit of the Act may solve some for some of these purposes, this is by no means a comprehensive solution.

Other exceptions are narrowed significantly. For instance,

a. Processing for mergers and acquisitions is now permissible under a broader exception[37], but only when the underlying scheme has been approved by a court or tribunal, thereby excluding private arrangements[38]; and

b. The exceptions for credit scoring[39] and fraud prevention[40] under the Draft, have now been consolidated into a narrow exception for ascertaining whereabouts, financial information and assets and liabilities of a person from whom a claim is due against a debt owed, and then in compliance with the relevant law.[41]

The omission and narrowing of the aforementioned types of exceptions which are common internationally,[42] and the removal of the mechanism through which additional "fair and reasonable" purposes could be specified,[43] is not only contrary to the general flexible, business friendly tone of the Act, but also may prove unwieldy in the years to come.

35 Section 8(7), Draft.
36 Section 8(8), Draft.
37 In comparison to Section 8(8)(b), Draft.
38 Section 17(1)(e), Act.
39 Section 8(8)(d), Draft.
40 Section 8(8)(a), Draft.
41 Section 17(1)(f), Act.
42 Section 6, Part 3, PDPA; Recital 47, GDPR.
43 Section 8(9), Draft.

Key Contacts:

Cyril Shroff
Managing Partner
cyril.shroff@cyrilshroff.com

Arun Prabhu
Partner (Head - Technology & Telecommunications)
arun.prabhu@cyrilshroff.com

Arjun Goswami
Director - Public Policy
arjun.goswami@cyrilshroff.com

Contributors:

Arun Prabhu
Partner (Head - Technology & Telecommunications)

Anirban Mohapatra
Partner

Arpita Sengupta
Senior Associate

Mahim Sharma
Senior Associate Designate

Anoushka Soni
Associate

Sabreen Hussain
Associate

Soumya Tiwari
Associate

Disclaimer

All information given in this alert has been compiled from credible, reliable sources. Although reasonable care has been taken to ensure that the information contained in this alert is true and accurate, such information is provided 'as is', without any warranty, express or implied as to the accuracy or completeness of any such information.

Cyril Amarchand Mangaldas shall not be liable for any losses incurred by any person from any use of this publication or its contents. This alert does not constitute legal or any other form of advice from Cyril Amarchand Mangaldas.

Should you have any queries in relation to the alert or on other areas of law, please feel free to contact us on cam.publications@cyrilshroff.com

Cyril Amarchand Mangaldas
Advocates & Solicitors

100+ years of legacy | **1000** Lawyers | **Over 170** Partners

Peninsula Chambers, Peninsula Corporate Park, GK Marg, Lower Parel, Mumbai 400 013, India
T +91 22 2496 4455 **E** cam.mumbai@cyrilshroff.com **W** www.cyrilshroff.com
Presence also in Delhi-NCR | Bengaluru | Ahmedabad | Hyderabad | Chennai | GIFT City | Singapore