IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

PROCESSING WITHOUT CONSENT: THE STRUCTURAL DEFICIENCIES OF INDIA'S LEGITIMATE USES FRAMEWORK UNDER THE DPDP ACT, 2023

Dr Ankit Raghuvanshi
Assistant Professor, Department of Law
Harish Chandra PG College, Varanasi

Abstract

The Digital Personal Data Protection Act 2023 declares consent to be the 'primary lawful basis for processing personal data'[1] then proceeds to create nine grounds on which processing can be done without it.[2] This is not, by itself, a problem. Every serious data protection framework contains consent-bypass provisions.[3] The problem with Section 7 of the DPDP Act is what it withholds from Data Principals whose data is processed under these grounds: no notice of the processing, no notice of the legal basis being invoked, and no right to object or challenge. Three of the nine grounds — voluntary disclosure under Section 7(a), State benefit delivery under Section 7(b), and employment under Section 7(i) — are drafted broadly enough that they operate not as narrow exceptions to the consent principle but as a parallel processing regime that it creates questions regarding the sanctity of the economically lucrative processing of data being done in India. The paper measures this framework against the GDPR's Article 6 architecture and the Supreme Court's proportionality doctrine from Puttaswamy, and finds it deficient on both counts. Four targeted reforms are proposed.[4][5]

[1] Digital Personal Data Protection Act 2023 (Act 22 of 2023) (India), s 6(1).

[2] Ibid, s 7.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) [2016] OJ L 119/1, Art 6(1).

[4] GDPR, Art 14 (requiring the controller, where data has not been obtained directly from the data subject, to provide information on the purpose and legal basis, the categories of data, and the source from which it was obtained).

[5] GDPR, Art 13 (notice obligation where data is collected directly from the data subject).

I. INTRODUCTION

There is a paradox at the heart of the DPDP Act 2023. Section 6(1) requires that processing of personal data be based on 'free, specific, informed, unconditional and unambiguous consent, signified by a clear affirmative action'[6] underlying the notion of free consent. Section 7 however goes on to establish nine grounds on which processing may proceed without any of that.[7] The Act calls these grounds 'certain legitimate uses.' What they actually are, in several instances, is a systematic licence to process data even where the Data Principal's knowledge, agreement, or any effective means of challenge are absent.

Consent-bypass grounds are a structural feature of every mature data protection framework. Processing for medical emergencies, legal obligations, and national security cannot realistically wait for individual consent. The GDPR has six lawful bases besides consent.[8] The argument here is not that Section 7 should not exist. It is that Section 7, as drafted, is deficient in two related respects that are not inevitable features of consent-bypass regimes but specific choices Parliament made — or failed to make.

The first deficiency is structural: Section 7 processing carries no notice obligation, no transparency requirement, and no right of challenge. A Data Principal has no way of knowing her data is being processed under Section 7, no way of finding out which ground is being invoked, and no statutory mechanism to contest it. The GDPR, by contrast, treats transparency as a prerequisite for every lawful basis, not just consent.[9][10] The second deficiency is in the drafting of three specific grounds, each of which is broad enough to displace consent not at the margin but at scale. The paper examines those three grounds in detail before turning to the constitutional framework and reform proposals.

II. MAPPING SECTION 7: NINE GROUNDS AND WHAT THEY LEAVE UNSAID

A brief map of all nine grounds is necessary before the analysis can proceed. The grounds range from the obviously necessary to the genuinely alarming, often in the same sentence.

Section 7(a) permits processing where a Data Principal has for a specified purpose, consensually provided their data and has not clearly specified that they do not consent to the processing of the same.[11] The illustrations suggest transactional contexts: a pharmacy sending a payment receipt, a real estate broker receiving contact details. The drafting is not so limited, for reasons examined in Part IV.

Section 7(b) permits the State and its associated instrumentalities to the processing of personal data with a view to provide subsidies, benefits, services, certificates, licences, or permits — either where the Data Principal has previously consented for any such purpose, or where the data is available in a State database

[6] Digital Personal Data Protection Act 2023, s 6(1).
[7] Ibid, s 7.
[8] GDPR (n 3), Art 6(1).
[9] GDPR, Art 14.
[10] GDPR, Art 13.
[11] Digital Personal Data Protection Act 2023, s 7(a).

which has been notified.[12] This ground covers the entire digital public infrastructure of India: Aadhaar-linked benefit delivery, digital health records, vehicle registration databases, and the National Population Register.

Section 7(c) permits processing of data in the interest of sovereignty, integrity, or security or under any law in force for the performance of functions of the State.[13] It has no limiting principle beyond the existing statute book, which means it is as broad as every law Parliament has ever passed that touches data.

Sections 7(d) and 7(e) cover disclosure obligations under Indian law and compliance with judicial orders respectively.[14][15] These are defensible and narrow. Tax filings, regulatory reporting, court-ordered disclosures: few would argue these require individual consent.

Sections 7(f), 7(g), and 7(h) cover medical emergencies, epidemic response, and disaster management.[16][17][18] Again, plainly defensible. The Disaster Management Act's definition of 'disaster' is broad,[19] which gives Section 7(h) more reach than its emergency framing suggests, but the core rationale is sound.

Section 7(i) is the employment ground. It permits processing of data for the purposes relating to employment or for protecting the employer from loss or liability, which could include instances of prevention of corporate espionage, instances relating to maintenance of confidentiality of trade secrets and also extends to classified information, further extending to include provision of any service or benefit sought by an employee.[20] This is the ground most likely to affect the most people, most of the time, in ways they do not know about and cannot contest. Part IV returns to it.

III. THE STRUCTURAL PROBLEM: THREE ABSENCES

The deeper problem with Section 7 is not any individual ground. It is the complete absence of three protections that the GDPR treats as prerequisites for any lawful processing, regardless of basis.

The first absence is notice. Section 5's notice requirement applies only to consent-based processing.[21][22] A Data Fiduciary that processes personal data under Section 7 owes the Data Principal nothing — no notification of the processing, no disclosure of the legal ground being invoked, no indication of what data is being used or for what purpose. A person whose employer is monitoring his communications under Section 7(i), or whose medical records are being shared between government databases under Section 7(b), has no

[12] Ibid, s 7(b).
[13] Ibid, s 7(c).
[14] Ibid, s 7(d).
[15] Ibid, s 7(e).
[16] Ibid, s 7(f).
[17] Ibid, s 7(g).
[18] Ibid, s 7(h).
[19] Disaster Management Act 2005 (Act 53 of 2005) (India), s 2(d) (defining 'disaster' to include natural and man-made calamities of a nature or magnitude that is beyond the coping capacity of the community of the affected area).
[20] Digital Personal Data Protection Act 2023, s 7(i).
[21] Digital Personal Data Protection Act 2023, s 5 (notice requirement applies only to consent-based processing under s 6; no equivalent provision applies to s 7 processing).
[22] Ibid, s 37 (read with s 5, confirming that the notice obligation is triggered only where processing is based on consent).

statutory duty on the Principal to inform or the right of the fiduciary to know about it. Under GDPR Article 14, where data of the subject has not been taken directly from them, the controller must still provide information on the categories of the data, the legal basis and the purpose, also the source from which it was obtained.[23] The DPDP Act has no equivalent. This is not a minor technical gap. It is the difference between a framework that treats Data Principals as participants in the legal relationship and one that treats them as objects of it.

The second absence is a Right of the data Principals to object or challenge such processing. Under GDPR Article 21, a data subject may object to processing for performance of a public task or processing based on legitimate interests, and the controller is required to demonstrate such compelling legitimate grounds that override the data subject's interests in order to resume such processing.[24] The DPDP Act contains no analogous right for Section 7 processing. The Data Principal's rights in Chapter III of the Act — access, correction, erasure, and grievance redress[25] — are framed in terms of consent-based processing. A Data Principal who discovers that her personal data has been processed under Section 7 has no specific statutory mechanism to challenge the processing itself, as distinct from seeking correction of inaccurate data.

The third absence is the most fundamental: there is no proportionality or necessity requirement anywhere in Section 7. The GDPR's legitimate interests basis requires a three-part balancing test: a legitimate interest must exist, the interest for processing and overriding the data subjects' interest should be a necessity, and the interest must subject's fundamental right should not be overridden.[2627] Section 7 of the DPDP Act requires none of this. Processing under Section 7(i) for 'safeguarding the employer from loss or liability' does not need to be the least restrictive means available to the employer. Processing under Section 7(b) does not require the demonstration on part of the State as to the processing being a necessity to demonstrate that the data it is processing is necessary for the specific benefit or service being delivered. The absence of a necessity requirement is not merely a gap in procedural protection. It is a failure of the Act's foundational commitment to privacy as a right rather than a privilege.[28]

IV. THREE GROUNDS UNDER THE MICROSCOPE

Three of the nine grounds warrant closer examination: Section 7(a) for its internal contradiction with Section 6(1), Section 7(b) for its implications in the Aadhaar ecosystem, and Section 7(i) for the power asymmetry it institutionalises.

[23] GDPR, Art 14 (n 4 above).

[24] GDPR, Art 21 (right to object to processing based on legitimate interests or the performance of a public task, placing the burden on the controller to demonstrate compelling legitimate grounds to continue).

[25] Digital Personal Data Protection Act 2023, ss 13, 14 (right to access information about personal data processed and right to correction and erasure).

[26] Article 29 Data Protection Working Party, 'Guidelines on Legitimate Interests' (wp217, 9 April 2014) 4 (setting out the three-part balancing test: existence of a legitimate interest, necessity of the processing, and non-override of the data subject's fundamental rights and interests).

[27] Article 29 Working Party, 'Guidelines on Legitimate Interests' (n 26 above) 6.

[28] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (Supreme Court of India).

Section 7(a)'s voluntary disclosure ground inverts the Act's own consent standard. Section 6(1) requires consent to be signified through a 'clear affirmative action.'[29] Section 7(a) permits processing where the Data Principal 'has not indicated that she does not consent' to the specified purpose for which she voluntarily provided her data.[30] One standard is opt-in. The other is opt-out. Both appear in the same Act, and together they govern the bulk of transactional data processing in the digital economy. In practice, nearly every user involves the voluntary provision of personal data during the interaction over a digital platform for a specified purpose: placing an order, registering an account, filling a form. Section 7(a) means that all of this falls outside the affirmative consent standard of Section 6(1), unless the Data Principal has somehow affirmatively indicated non-consent. How she is supposed to indicate non-consent when she has received no notice of the processing is a question the Act does not answer.[31] The Srikrishna Committee's 2018 report had flagged this risk explicitly, recommending that any voluntary disclosure ground be accompanied by clear purpose specification at the point of collection.[32] That recommendation did not survive into the final Act.

Section 7(b) and its interaction with the Aadhaar ecosystem requires careful reading. The ground permits State processing where a Data Principal has previously consented 'for any subsidy, benefit, service, certificate, licence, or permit' offered by the State.[33] The word 'any' is doing significant work here. It suggests that prior consent for one government service may activate the ground for all government services. A person who enrolled in a food subsidy scheme in 2016 may, on the plain reading of Section 7(b), have provided the consent that makes her data available for processing across the State's entire data infrastructure. This is precisely the concern the Supreme Court addressed in the Aadhaar judgment: that a single act of enrolment into a government programme cannot be treated as consent to indefinite downstream processing across unrelated purposes.[34][35] For reasons of permitting private entities to use Aadhaar authentication without adequate safeguards Section 57 of the Aadhaar Act was struck down.[36] Section 7(b) does not repeat that specific error — it applies to State processing only — but it risks replicating the underlying logic: that a historic consent, given in a specific transactional context, can be repurposed indefinitely by the entity that received it.

[29] Digital Personal Data Protection Act 2023, s 6(1) (requiring consent to be 'signified through a clear affirmative action').

[30] Ibid, s 7(a) (permitting processing where the Data Principal 'has not indicated that she does not consent' to the specified purpose for which she voluntarily provided her data).

[31] Eleni Kosta, Consent in European Data Protection Law (Martinus Nijhoff Publishers, Leiden, 2013) 208 (arguing that the distinction between 'opting in' and 'failing to opt out' is not a technical distinction but a political one, reflecting competing assumptions about the default relationship between citizens and data processors).

[32] Justice B.N. Srikrishna (Chair), A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, 2018) 47 (recommending that any voluntary disclosure ground be accompanied by clear purpose specification at the point of data collection).

[33] Digital Personal Data Protection Act 2023, s 7(b) (permitting State processing where the Data Principal has previously consented 'for any subsidy, benefit, service, certificate, licence, or permit' offered by the State or any of its instrumentalities).

[34] Justice K.S. Puttaswamy v Union of India (Aadhaar) (2019) 1 SCC 1 (Supreme Court of India).

[35] Usha Ramanathan, 'A Unique Identity Bill' (2010) 45(21) Economic and Political Weekly 10, 13 (warning that broad State data processing powers built on historic or implied consent create conditions for 'consent laundering' in which a single enrolment into a government programme authorises indefinite downstream processing).

[36] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (Act 18 of 2016) (India), s 57 (struck down in Puttaswamy (Aadhaar) (n 34) paras 301-310 as unconstitutional to the extent it permitted private entities to use Aadhaar authentication without adequate safeguards).

Section 7(i) is the employment ground, and it is the most legally troubling of the nine. The employer and employee relatationship is characterised structurally by power asymmetry. An employee cannot freely negotiate the terms on which her personal data is processed by her employer. This is not a fringe academic observation. It is the reason the GDPR's Recital 43 explicitly identifies employment relationships as a situation where the valid legal ground for processing can be provided by consent.[37] The DPDP Act, by placing employment processing entirely outside the consent framework and without any proportionality requirement, does something the GDPR deliberately avoids: it makes the employment relationship a zone of effectively unregulated data processing.[38]

The corporate espionage carve-out in Section 7(i) is particularly broad. Processing for 'prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information' is permitted without notice to the employee, without any requirement of questioning the proportionality of the specific risk being managed, and without any right of challenge.[39] An employer who monitors all employee communications on the basis that some employees might be leaking trade secrets is, on the drafting of Section 7(i), acting lawfully. An employee who suspects this is happening has no DPDP Act mechanism to find out whether it is, let alone to contest it. This is not a gap at the margins. It is a gap in the centre of the framework.

V. THE GDPR COMPARATOR: THREE STRUCTURAL DIFFERENCES

The GDPR's six lawful bases in Article 6(1) are the most relevant comparator for Section 7.[40] Three structural differences stand out, each corresponding to one of the absences identified in Part III.

The first difference is transparency parity. Under the GDPR, every lawful basis — including legitimate interests — triggers the Article 13 or Article 14 notice obligation.[41][42] A data subject always knows the legal basis on which her data is being processed, even if she has not consented to it. Article 14's notice obligation for indirectly obtained data specifically addresses the scenario most analogous to Section 7 processing: the controller has obtained data without a direct consent transaction and must still tell the data subject what it has, why, and on what basis.[43] The DPDP Act's Section 7 processing happens in complete informational darkness from the Data Principal's perspective. She may have rights on paper. She has no way to exercise them.

[37] GDPR, Recital 43 ('Consent should not provide a valid legal ground for processing where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority').

[38] Nishtha Jaswal and Prashant Kumar, Data Protection Law in India (LexisNexis, New Delhi, 2023) 122 (observing that s 7(i)'s corporate espionage carve-out is 'drafted more broadly than any equivalent provision in the GDPR or the UK GDPR').

[39] Digital Personal Data Protection Act 2023, s 7(i).

[40] GDPR (n 3), Arts 6(1)(b)-(f) (processing necessary for performance of a contract, legal obligation, vital interests, public task, and legitimate interests respectively).

[41] GDPR, Art 14 (n 4 above).

[42] GDPR, Art 13 (n 5 above).

[43] Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law and Security Review 179, 190 (arguing that transparency parity across all lawful bases is a structural prerequisite for any effective data subject rights regime).

The second difference is the legitimate interests balancing test. GDPR Article 6(1)(f) requires a documented three-part assessment: legitimate interest, necessity, and non-override of the data subject's rights.[4445] Authorities involved in Data Protection across Europe have developed detailed guidance regarding the application of this test. As a result, legitimate interest processing is not arbitrary but a documented decision that can be reviewed by regulators and challenged by data subjects. Section 7 of the DPDP Act contains no equivalent balancing requirement for any of its nine grounds. The Data Fiduciary's assessment of whether a Section 7 ground applies is, at present, self-certified and unreviewable.

The third difference is the right to object. Article 21 provides a right to the data subjects exercising which they could object to processing of data based on legitimate interests or public tasks, requiring the controller to produce compelling reasons before they could continue.[46] This right has teeth: it is enforced, it is the subject of DPA guidance, and it provides a practical remedy for the individual. The same cannot be said by DPDP Act's Chapter III dealing with rights which includes, access, correction, erasure, grievance redress, largely forming parts of procedural rights regarding how data is handled, not substantive rights to contest why it is being processed at all.[47] The absence of a right to object to Section 7 processing represents, as Bhandari and Rahman have observed, a regression from the 2019 Personal Data Protection Bill's approach, which had included a purpose limitation principle applicable across all processing grounds.[48]

VI. THE CONSTITUTIONAL DIMENSION: SECTION 7 AND PUTTASWAMY PROPORTIONALITY

Puttaswamy established that any interference made with the right to privacy under Article 21 must satisfy a four-part proportionality test which includes legality, legitimate aim, necessity, and procedural guarantees against abuse.[49] The Maneka Gandhi principle of substantive due process reinforces this stating that a law affecting personal liberty must be fair, just, and reasonable in its content, not merely in its form.[50]

Section 7 satisfies the legality limb without difficulty — it is a provision of an Act of Parliament. Most of the nine grounds also satisfy the legitimate aim limb: State security, medical emergencies, and judicial compliance are plainly legitimate. The framework is vulnerable on the third and fourth limbs.

[44]GDPR, Art 6(1)(f) (legitimate interests basis, requiring the controller's interests not to override the data subject's fundamental rights and interests, having regard in particular to whether the data subject is a child).

[45]Article 29 Working Party, 'Guidelines on Legitimate Interests' (n 26 above) 7.

[46]GDPR, Art 21 (n 24 above).

[47]Digital Personal Data Protection Act 2023, ss 13, 14 (n 25 above).

[48]Vrinda Bhandari and Faiza Rahman, 'Understanding India's Data Protection Framework' (2024) 56 Journal of the Indian Law Institute 1, 17 (noting that the absence of a right to object to s 7 processing represents a regression from the 2019 Personal Data Protection Bill, which had included a purpose limitation principle applicable across all processing grounds).

[49]Puttaswamy (n 28), para 325 (Chandrachud J) (identifying legality, legitimate aim, necessity, and proportionality stricto sensu as the four limbs of the constitutional proportionality test in the privacy context).

[50]Maneka Gandhi v Union of India AIR 1978 SC 597 (Supreme Court of India) (holding that a law affecting personal liberty under Art 21 must be fair, just, and reasonable in its content, not merely in its form).

The necessity while achieving the legitimate aim requires that the interference be least restrictive.[51] Section 7 imposes no necessity requirement on Data Fiduciaries invoking its grounds. An employer who processes all employee communications under Section 7(i) need not demonstrate that targeted, purpose-specific monitoring would be insufficient to address the risk. A government department that processes a citizen's entire health history under Section 7(b) need not demonstrate that a narrower category of data would not suffice. In a situation where the statutory necessity requirement is absent would imply that under Section 7 processing can be as broad as the Data Fiduciary chooses, without any obligation to justify that breadth.

The procedural guarantee limb is where Section 7 fails most completely. Puttaswamy required that privacy-invasive measures be accompanied by 'procedural safeguards against the abuse of the interference.'[52] In the context of a statutory data processing scheme, the minimum requirement includes: notice to the affected person, an opportunity to be heard, and a mechanism for independent review. Section 7 provides none of these. The Data Principal does not know that their data is being processed, does not know why, and has no means of challenge. The Aadhaar judgment applied this logic to State welfare processing specifically, holding that even data processing for legitimate public purposes must be accompanied by adequate procedural safeguards.[53] Section 7(b)'s State processing ground is directly in the frame of that holding.

The proportionality analysis in Modern Dental College adds the requirement that the interference be proportionate in the strict sense: the benefits of the measure must not be outweighed by the severity of the restriction on rights.[54] For Section 7(i)'s employment ground, this test is difficult to pass. The benefit to the employer of unnoticed, unconstrained employee monitoring is real but not unlimited. The cost to the employee — the systematic erosion of privacy in the workplace, without knowledge or recourse — is substantial. A court asked to weigh those interests, in the absence of any statutory proportionality analysis, would be doing the work Parliament chose not to do.

VII. REFORM PROPOSALS AND CONCLUSION

Four targeted reforms would address the structural deficiencies identified in this paper without requiring wholesale reconstruction of Section 7.

First, Section 7 processing must be subject to a minimum notice obligation. The Act should be amended to require Data Fiduciaries invoking any grounds under Section 7 would require notification to the Data Principal regarding the ground ground for invocation, the category under which the data falls which is being processed, further specifying the purpose for which it is used, this would be modelled as per GDPR

[51] Puttaswamy (n 28), para 310 (Chandrachud J) ('Necessity requires that the measure adopted is the least intrusive means to achieve the legitimate aim').

[52] Puttaswamy (n 28), para 325 (Chandrachud J) (requiring that privacy-invasive State measures be accompanied by procedural safeguards against the abuse of the interference).

[53] Justice K.S. Puttaswamy v Union of India (Aadhaar) (n 34), para 239 (Sikri J) (holding that even data processing for legitimate public welfare purposes must be proportionate and accompanied by adequate procedural safeguards).

[54] Modern Dental College and Research Centre v State of Madhya Pradesh (2016) 7 SCC 353, paras 40-42 (Supreme Court of India, adopting the four-part proportionality test and requiring that the benefits of a measure not be outweighed by the severity of the restriction on fundamental rights).

Article 14.[55] The notification need not be pre-processing in all cases: medical emergencies and disaster response cannot wait. But it should be provided as soon as reasonably practicable after processing begins, and before the data is used for any secondary purpose.

Second, Section 7(i) must be amended to include an explicit proportionality requirement. Employment processing must be exercised in a limited manner and strictly for the stated purpose, blanket surveillance justified by the corporate espionage carve-out should be prohibited unless the employer can demonstrate a specific, documented risk that less intrusive measures are insufficient to manage.[56]

Third, Section 7(a) must be redrafted to eliminate the internal contradiction with Section 6(1). Voluntary disclosure processing should require clearly stating the purpose at the point where the data is collected futher a specified mechanism by which the Data Principal may indicate non-consent.[57] The current drafting which permits processing unless the Data Principal has 'indicated' non-consent she does not know she has the right to indicate, is not a workable standard.[58]

Fourth, a right to object to Section 7 processing should be introduced in Chapter III of the Act, modelled on GDPR Article 21,[59] allowing Data Principals to challenge processing under Section 7 grounds where for the stated purpose, the processing of data is not necessary or where their fundamental rights override the Data Fiduciary's legitimate interest. The burden of justification should lie with the Data Fiduciary, not the Data Principal.

The DPDP Act 2023 did something that needed doing: it gave India a statutory data protection framework. Section 7's nine legitimate uses grounds are, for the most part, grounds that needed to be there. The problem is the company they keep — or rather, the protections they have been allowed to travel without. Notice costs something. A right of objection costs something. A proportionality requirement costs something. Those costs fall on Data Fiduciaries who would prefer the freedom to process without accounting for it. They are costs that a framework serious about privacy as a fundamental right must be willing to impose.

The consent principle is only as strong as the exceptions it can contain. Section 7, as currently drafted, does not contain its exceptions. It advertises consent as the governing standard and then displaces it, quietly, for the bulk of data processing that actually matters. That is not a careful calibration of competing interests. It is a structural evasion — and it deserves to be called one.

[55]GDPR, Art 14 (n 4 above) (the notification need not precede processing in every case; Art 14(3) permits delay where the data is used to communicate with the data subject, up to first communication, or where disclosure to third parties is contemplated, before that disclosure).

[56]Digital Personal Data Protection Act 2023, s 7(i) (n 20 above); Srikrishna Report (n 32) 49 (recommending that employment processing be limited to what is strictly necessary for the stated purpose and subject to a documented proportionality assessment).

[57]Digital Personal Data Protection Act 2023, s 6(1) (n 6 above) (requiring consent to be signified through a 'clear affirmative action'; the affirmative action standard is incompatible with the opt-out non-objection standard in s 7(a)).

[58]Ibid, s 7(a) (n 11 above) (permitting processing where the Data Principal 'has not indicated that she does not consent'; no mechanism is specified by which such indication may be made).

[59]GDPR, Art 21 (n 24 above) (the right to object applies at any time and must be explicitly brought to the data subject's attention at the latest at the time of first communication; the controller bears the burden of demonstrating compelling legitimate grounds to override the objection).