Major differences between the Personal Data Protection Bill, 2019 & GDPR

Topic	GDPR	Bill
Processing data	The legal bases on which personal data may be processed are (a) consent of the data subject (b) performance of contract to which the data subject is party (c) compliance with legal obligation of data controller (d) protecting vital interests of data subject (e) performance of a task carried out in the public interest (f) legitimate interests pursued by the controller or third party (Article 6(1))	The legal bases on which personal data may be processed are (a) consent of data principal (b) compliance with legal obligation (c) medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual (d) medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health (e) measures to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order (f) employment purposes (g) such reasonable purpose as specified by regulations to be notified by DPA (Sections 11 - 14) Significantly, performance of a contract and legitimate interests basis are *not* grounds for processing data without consent. Organisations rely on these two grounds for a wide range of activities which require consent under the Bill.
Registration of significant data fiduciaries	No requirement for registration	Significant data fiduciaries are required to register with the DPA as per the regulations (Section 26(2)) and comply with greater additional accountability requirements
Data localisation	There is no data localization requirement	Sensitive personal data must be stored in India but may be transferred outside India if there is explicit consent and if transfer is part of a DPA-approved contract or intra-group scheme for transfer or if the Indian government has deemed a country or class of entities to be providing adequate protection (Section 34(1)). Critical personal data must be processed only in India, except under emergency situations or where the Indian government approves (Section 34(2))
Anonymized data	Anonymized data falls outside the scope of GDPR.	The Indian government may, in consultation with the DPA, direct any data fiduciary to provide anonymized data "*to enable better targeting of delivery of services or formulation of evidence-based policies*" (Section 91(2))