Private and confidential
December 15, 2022

Comments on the Draft Digital Personal Data Protection Bill, 2022

By email

On November 18, 2022, the Indian Ministry of Electronics and Information Technology ("**MEITY**") released a draft Digital Personal Data Protection Bill, 2022 ("**Draft Bill**"). As part of the pre-legislative consultation process, the MEITY has invited comments on the Draft Bill from stakeholders. We welcome the opportunity to provide our views on the Draft Bill and participate in the legislation building process. **Our comments are set out in the table below.**

Section No.	Subject Matter	Comments
Amendments - Section 30	*(1) The Information Technology Act, 2000 ("**IT Act**") shall be amended in the following manner:* *(a) section 43A of the IT Act shall be omitted;* *(b) In section 81 of the IT Act, in the proviso, after the words and figures "the Patents Act, 1970", the words "or the Digital Personal Data Protection Act, 2022" shall be inserted; and* *(c) clause (ob) of sub-section (2) of section 87 of IT Act shall be omitted.*	**There may be clarity needed on whether the 2011 Privacy Rules are now superseded, or continue to apply in some form.** **The omission of sections of the IT Act under whose authority existing Privacy Rules have been issued may not cease the operation of these rules. To prevent regulatory confusion and discrepancy, the provision should clarify that any rules issued under the omitted sections shall not remain in force after enforcement of the 2022 Bill.** a. Presently, Section 30 *omits* sections (viz., 87(2)(ob) and 43A) of the IT Act under which the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Privacy Rules**") had been issued. We understand that the intent of this provision is to consequentially cease the existence of the Privacy Rules. However, this provision would not achieve this intent. Multiple supreme court rulings[1] have upheld the interpretation that an express omission constitutes to be a "repeal" as per the General Clauses Act, 1897 ("**Clauses Act**"). b. Section 24 of the Clauses Act states any rule issued under a repealed provision shall "*continue in force, and be deemed to have been made or issued under the provisions so reenacted, unless and until it is superseded by any appointment notification, order, scheme, rule, form or bye-law, made or issued under the provisions so re-enacted*". If the Draft Bill is enforced as is, the Privacy Rules will continue to exist in parallel, to

[1] *Shree Bhagwati Steel Rolling Mills* vs. *Commissioner of Central Excise and Ors.,* (2016) 3 SCC 643; *Fibre Boards (P) Ltd*., *Bangalore* vs. *Commissioner of Income Tax, Bangalore* (2015) 10 SCC 333.

Section No.	Subject Matter	Comments
		the extent that it is consistent with the Draft Bill. Although the Privacy Rules and Draft Bill are largely coterminous, it shall create duplicity of compliances. Please consider that, where an activity is already regulated, it should not have to undertake compliances under other laws.
Applicability - Section 4(1) and (2)	*The Draft Bill applies to* *(1) processing of digital personal data **within India;** and* *(2) processing of personal data outside India, if it is in connection with any profiling or offering goods and services to individuals within India.*	**The extra-territorial applicability of 2022 Bill may conflict with its stated objectives. Absent necessary clarifications it may (unreasonably) burden Indian entities and overseas entities and result in multiplicity of compliances.** a. As per Section 4(1) of the Draft Bill, it appears that the 2022 Bill will apply to any individual's personal data processed in India, irrespective of them being an Indian national or residing in India. Consequently, foreign personal data processed by Indian data fiduciaries in India would be regulated by the 2022 Bill. Please note that Indian entities process foreign personal data for various purposes, such as processing employee data of overseas parent company or alternatively for provision of services to individuals located outside India. Since the processing of a foreigner's personal data will (likely) already be regulated in the jurisdiction where such foreigner resides, Indian entities will have to undertake compliances under two set of laws. Adding language clarifying that the 2022 Bill shall only apply to processing of personal data of individuals located in India would prevent Indian companies from incurring incremental compliance costs. b. In the same vein, Section 4(2) does not contemplate that in certain instances individuals located in India may access platforms based overseas ("**overseas platforms**"). Such platforms may not actively be offering their platforms in India and may have been accessed by individuals in India by virtue of pervasiveness of the Internet. However, based on the current language of Section 4(2), the availability of an overseas platform in India would qualify as offering goods / services in India. We recommend restricting the applicability of this 2022 Bill only to instances where (a) such offering is "*targeted*" or (b) if the individual in India avails the service / good provided via such overseas platform.

Section No.	Subject Matter	Comments
Cross-Border Data Transfers - Section 17	*The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.*	**Proposed cross-border 'white-listing' mechanism may impede businesses dependent on flows of data. Like other global privacy legislations, offering multiple transfer tools will be a step towards improving ease of doing business in India.** a. The simplification of the mechanism for permitting cross-border data transfers is welcome. As per the proposed mechanism, the Central Government will notify the countries to which personal data may be transferred. Pending such notification, transfer of personal country anywhere outside India shall be restricted, and in-turn be restrained to store data locally; halting all forms of personal data may not be practically feasible. Please consider alternatively opting for an approach similar to that for foreign investments; except for specified prohibited countries, and subject to sectoral conditions, investments are permitted from all countries[2]. Accordingly, we suggest revising Section 17 to state that data fiduciaries and data processors may permit personal data outside India except to jurisdictions expressly prohibited by the Central Government[3]. b. Relying solely on an assessment-based mechanism for cross-border transfers may negatively impact businesses and operation of internet platforms. For instance, if the list of countries permitted by the Data Protection Board ("**Board**") are challenged before the Supreme Court ("**SC**") and such list is 'stayed' by the SC, it may cause a stand-still for all cross-border data flows. To ease the onus placed on the Board, additional grounds in line with global practices can be specified, such as: 1. **Standard-contractual**[4]: The European Commission issued a set of contractual clauses which ensures appropriate data protection safeguards are accorded to

[2] Chapter 3 of the Consolidated Foreign Direct Investment Policy, 2020.

[3] In addition to cross border transfer grounds provided under the GDPR, MEITY may consider referring to the approach towards cross-border data transfer opted by Argentina (Law No. 25,326 of Personal Data Protection) and Brazil (General Data Protection Law, Federal Law No. 13,709/2018). Under these legislations, transfers are (inter alia) permitted if the data subject provides "specific and highlighted" consent for the transfer with prior information about the international leg of processing, clearly distinguished from the purposes and for carrying out contractual obligations, to which a data subject is a party, at the request of the data subject.

[4] On June 04, 2021, the European Commission released the final version of two sets of standard contractual clauses ("**SCCs**") for – (a) use between controllers and processors[4]; and (b) transfer of personal data to third countries that do not meet General Data Protection Requirements ("**GDPR**") for an adequate level of data protection.

Section No.	Subject Matter	Comments
		personal data transferred outside the European Union. "Model Contracts" may be issued for entities to adopt for data transfers outside India. 2. **Binding Corporate Rules approved by the Board**[5]: These are data protection policies adhered to by companies established for transfers of personal data outside their jurisdiction within a group of undertakings or enterprises. Entities may submit their binding corporate rules for approval by the Board. 3. **Third Country Laws Assessment**[6]: The European Data Protection Board adopted a six-step process for organizations to carry out prior to transferring personal data to third countries (countries outside the European Economic Area (EEA)). India's Board may also formulate a similar process to facilitate data transfers outside India, with obtaining requisite representations from the entity transferring data outside India. 4. **Contractual obligations**: A data fiduciary or data processor's obligations towards a data principal may require it to transfer personal data outside India.
Itemized Notice – Section 6(3)	*The itemized notice to be provided to a data principal prior to commencement of processing their personal data and after obtaining consent should be made available in English or any language specified in the Eighth Schedule to the Constitution of India ("**Schedule 8**").*	**Implementing tools to provide notices and privacy policies in twenty or more languages may not be feasible for overseas entities.** **Noting the linguistic diversity of India, entities should only be required to undertake such translations in specific cases, and not mandate providing these.** a. It is unclear if the notice(s) are to be made available in English *or* any of the 22 languages listed under Schedule 8. In our view, by default, the notice should be provided in English, *and* in any other language only if a data principal requests such information in the said language. Please consider that it may not be (commercially and operationally) viable for small-scale overseas (and Indian) entities to carry out translation of notices in 22 regional languages, and update each such notice in the

[5] Article 47 of the GDPR.
[6] On November 10, 2020, and June 18, 2021, the European Data Protection Board adopted two sets of measures that are supplement transfer tools to ensure compliance personal data transferred to a third country is accorded essentially equivalent level of protection of personal data, as provided in the European Union. These measures include SCCs and a six-step process for organizations to carry out prior to transferring personal data to third countries (countries outside the European Economic Area (EEA)), in order to assess the level of data protection offered by the third country and its adequacy

Section No.	Subject Matter	Comments
		event of changes to processing activities. This will lead to an unconscionable compliance burden, and may also lead to 'terms arbitrage' between different interpretations of the same term. b. We note that the recent amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, also require intermediaries to publish policies and agreements pertaining to its platform in English or the Schedule 8 languages. As such, the intermediaries may, at its discretion, choose to provide the agreements, etc., in languages besides English. Similarly, Section 6(2) should be revised to reflect that the facility of perusing notices under other languages shall be provided at the sole discretion of the data fiduciary, and not a mandatory obligation.
Deemed Consent – Section 8	*The provision sets out the grounds on which a data fiduciary may process personal data without obtaining express consent of the data principal, and is deemed to have obtained her consent, for such ground.*	**The inclusion of deemed consent as a basis for processing personal data is a welcome step. Incorporation of additional grounds, and modifications suggested will enhance the effectiveness of this provision.** a. We appreciate the introduction of the concept of "deemed consent". Presently, this provision allows data fiduciaries to process personal data of a data principal without their consent, if the purpose for such processing satisfies any of the grounds set out under this provision. While a wide set of instances have been identified, these may be updated to include processing for performing contractual obligations towards the data principal (that is, deemed consent under a valid contract), complying with statutory requirements (in addition to judicial functions), and internal transfers between group companies. b. From a practical standpoint, carrying out processing pursuant to a contract may be covered under Section 8(1) (viz., processing when it is reasonably expected that the data principal shall provide their personal data). However, express recognition of processing for contractual obligations will allow businesses to undertake these operations, without having to demonstrate the legitimacy of such processing, unless required.

Section No.	Subject Matter	Comments
		c. Various laws applicable to a business involves reporting of information, which may invariably include personal data of its customers. Procuring consent of each data principal prior to such reporting may not be feasible; failure/ delay in furnishing information could result in imposition of penalties upon data fiduciaries for. As such, compliance with extant laws should also be specified as a ground for processing personal data without the consent of data principals[7]. d. Apart from the inclusion of additional grounds, please consider if the phrase "public interest" can be deleted from Section 8(8). The grounds identified under this sub-section may not fall within the ambit of the definition of public interest provided under Section 2(18) of the Draft Bill. For instance, since mergers and acquisitions of a body corporate do not relate to public interest *per se*, data fiduciaries may be constrained to obtain consents of the data principals for such activities. e. Section 8(9) enables processing of personal data for "***fair and reasonable purposes***", subject to certain factor, including the legitimate interests of the data fiduciary. The inclusion of "***legitimate interests***" is in conformity with global privacy legislations. However, we recommend carving out legitimate interest of a data fiduciary be as a standalone ground for deemed consent, as opposed to treating it as a factor to ascertain whether the data fiduciary's purpose for processing is fair and reasonable. Instead of determining what is considered *fair and reasonable,* the Board may, on a continuing basis, identify activities that would be considered as a legitimate interest. f. On a related note, Section 9(9)[8] of the Draft Bill requiring data fiduciaries to obtain the consent of data principals for engagement of data processors should also be suitably revised and aligned that such consent may be deemed to have been granted, pursuant to data fiduciary's contractual obligations towards data principals in accordance with the grounds for deemed consent under Section 8.

[7] Presently, Section 8(3) of the Draft Bill states that deemed consent is permitted only *for compliance with any judgment or order issued under any law.*

[8] The Data Fiduciary may, where consent of the Data Principal has been obtained, share, transfer or transmit the personal data to any Data Fiduciary, or engage, appoint, use or involve a Data Processor to process personal data on its behalf, only under a valid contract. Such Data Processor may, if permitted under its contract with the Data Fiduciary, further engage, appoint, use, or involve another Data Processor.

Section No.	Subject Matter	Comments
Personal Data Breach – Section 9(5)	*In the event of a personal data breach, the data fiduciary or data processor, as the case may be, is required to notify the Board and each affected data principal.*	**Notifying *every* personal data breach may trivialize sensitivity. Considering the technical challenges involved, stakeholder inputs should be sought prior to prescribing norms for reporting personal data breaches.** a. The requirement to notify each affected data principal for any personal data breach appears to be onerous. In certain instances, the IT systems of a data fiduciary may be impacted; however, the harm caused to the data principal may be notional / insignificant. Further notifying the Board of each breach, despite the lack of any severity or potential harm to stakeholders involved, may not serve any actual purpose. For preventing undue concerns and panic, notification requirements should be limited to breaches that merit the attention of the Board and/or data principals. b. Further obligating data processors to notify each personal data breach may not be within their remit. Since the data fiduciaries are better placed to ascertain the actual impact of a breach, responsibility to notify the Board and/or data principals should be limited to them. Note that, requiring data processors to notify the data principals may also result in inadvertent leakage of personal data. Alternatively, the provision may be revised to require that data processors should notify data fiduciaries in the event of a breach, irrespective of a contrary agreement to that effect. c. We note that the format for the personal data breach will be prescribed via subordinate legislation. Prior to prescribing the norms of reporting personal data breaches, please consider seeking stakeholder inputs on the technical feasibility for reporting of breaches, timelines, and the manner in which it is to be reported.
Data Processor rights – Section 9	*The provision sets out the obligations of a Data Fiduciary and exceptions to such obligations.* *Data fiduciaries must cease to retain personal data if (a) the purpose for*	**Exemptions accorded to data fiduciaries have not been extended to data processors. Provision specifying a data processor's degree of responsibility and decision making towards data processed by them will clarify potential confusion regarding the distinction between a data fiduciary and data processor.**

Section No.	Subject Matter	Comments
	which it was collected is no longer being served and (b) it is no longer necessary for legal or business purposes.	a. The Draft Bill does not detail the role of a data processor. It holds the data fiduciary to be responsible for compliance with the Draft Bill, including for any processors engaged by them[9]. However, certain rights available to data fiduciaries have not been extended to data processors. For instance, Section 9(6) clarifies the circumstances where retention of the personal data may be ceased. As per Section 9(6)(2), a data fiduciary may cease to retain data, unless such data is required for legal or business purposes; the rationale behind exclusion of data processors from availing this exemption is unclear. Please note that there may be scenarios where data processors would have to retain personal data processed by them (for e.g., Government data access requests, billing records reconciliation with data fiduciaries, etc.). For consistency, the facility to retain personal data for legal and business reasons should be extended to data processors as well[10]. b. On the other hand, there may also be instances where data processors may undertake actions on their own accord, which may be contrary to their arrangement with the data fiduciary. A provision setting out the extent of a data processor's role and clarifying that their activities shall be solely as per the instructions of the data fiduciary will afford protection to data fiduciaries, in the event of an unauthorized action taken by the data processor. Guidelines may be issued which details the relationship between data fiduciaries and data processors (for instance, steps in case of a personal data breach, sharing proof of consents, data retention for legal requirements, etc.)[11].

[9] Section 9(1) of the Draft Bill.

[10] In connection with Section 9(6)(2) of the Draft Bill, Section 13(2) accords the right to erasure should also be correspondingly revised to clarify that the destruction of data will be to the extent feasible, subject to the standards of deletion/data retention set out under Section 9(2). In the absence of any clarification, it may be construed that an exercise of right to erasure would require a data fiduciary to destroy all personal data relating to such individual, undermining their right to retain such data for legal / business reasons.

[11] Article 28 of the GDPR details the written contract between a data controller and data processor. It expressly states that the data processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required under law.

Section No.	Subject Matter	Comments
Child's Personal Data – Section 9(3) **and Definition of child –** Section 2(3)	*A "child" means an individual who has not completed eighteen years of age.*	**Age of classification as a child should be reduced to individuals aged between thirteen and sixteen years. Given the unbridled use of internet by all age groups and platforms particularly catering to children, threshold of eighteen years to accord one's own consent is not feasible, and contradictory to global data privacy laws.** a. Indian laws typically follow Indian Majority Act, 1875[12], to classify individuals as "minor" or "major". Given that children aged below eighteen years access Internet platforms and use their personal data to avail services such as academic content, *edu-tech* facilities, etc., resorting to the *age-gating* of eighteen may not fit. Note that, the age of classification under other global privacy laws ranges between thirteen to seventeen years[13]. It is common for businesses to record time spent by a child on a platform and provide details of their activity to their parents / guardians. As such, exemptions to Section 9(3) should be provided to ensure that business catering to children are not unduly hindered[14].
Financial Penalties – Section 25 and Schedule 1	*The penalties for various non-compliances under the Draft Bill ranges from INR Ten Thousand to INR 250 Crores. In aggregate, the penalty levied on a single entity for multiple non-compliances has been restricted to INR 500 Crores.*	**Financial penalties should be commensurate with other Indian laws. Excessive penalties may disincentivize overseas entities from participating in the Indian digital ecosystem.** a. The removal of criminal penalty for non-compliances with data privacy obligations is a progressive step. However, the proposed penalties are substantially higher than those typically specified under Indian legislations. For instance, the Consumer Protection Act, 2019 imposes a maximum penalty of INR 50 Lakhs[15], and allows a consumer to seek compensation proportionate to harm caused to them. Even the recently issued draft Indian Telecommunications Bill, 2022[16] contemplates penalty of up to INR 5 Crores. For completeness, the penalties under the Draft Bill are higher

[12] Section 3(1) of the Indian Majority Act, 1875, states that "*Every person domiciled in India shall attain the age of majority on his completing the age of eighteen years and not before*".
[13] Thirteen to Sixteen under the GDPR; Fourteen under South Korea's Personal Information Protection Act 2011, Thirteen under the California Consumer Privacy Act; Seventeen under the proposed American Data Privacy and Protection Act; and Thirteen under UK's Data Protection Act, 2018.
[14] Please note that a blanket prohibition of this nature may infringe the right to practice any profession accorded under Article 19(1)(g) of the Constitution of India, 1950.
[15] Section 89 of the Consumer Protection Act, 2019.
[16] Section 47, Schedule 3 and Schedule 4 of the Draft Indian Telecommunications Bill, 2022.

Section No.	Subject Matter	Comments
		than penalties prescribed globally for data privacy breaches. Since the intent of the Draft Bill is to safeguard the privacy of individuals and recompense them for harm done, the proposed penalties are excessive. Please consider realigning the penalties.
Right to grievance redressal – Section 14(2)	*A data principal is entitled to register a complaint with the Board if they are not satisfied with the response of a Data Fiduciary to a grievance or receives no response within seven days.*	**The current language of this provision creates the perception that all grievances are to be resolved within seven days. It should be revised to clarify that the seven day timeline is limited to acknowledging the grievance.** a. It is not clear if the seven-day timeline applies to resolution of a data principal's grievance or acknowledging the receipt of such grievance by the data fiduciary. In our view, this provision denotes that a data principal may escalate their grievance to the Board if they are not satisfied with the resolution or if the data fiduciary fails to acknowledge it within seven days of receiving it. To prevent ambiguity, the provision should be revised to clarify that the data fiduciary is required to acknowledge grievance(s) within seven days of receiving it. b. Thereafter, a 'sliding scale' can be prescribed for addressing grievances. While crucial issues such as personal safety can be prioritized, due course requests and queries can be dealt with on more relaxed timelines. These can be reflected in prescribed timelines under codes of conduct issued by the Board, for example.
Subordinate Legislation – Section 26	*The Central Government may, by, notification make Rules consistent with the provisions of the Draft Bill to carry out its provisions.*	**Pre-legislative consultations are an integral element of democratic processes. Over the past years MEITY has issued legislations only after seeking stakeholder inputs. For alleviating stakeholder concerns, it may be good practice to statutorily stipulate this.** a. A number of operational elements of the Draft Bill have been reserved for subordinate legislation to be issued by the central government, such as cross-border data transfers, treatment of children's personal data, etc. Section 26 presently does not contemplate carrying out a pre-legislation consultation process. Given the dynamic nature of technologies and diverse business models, it would be prudent to involve stakeholders prior to formulation of subordinate legislations.

Section No.	Subject Matter	Comments
Stage-Wise Implementation – Section 1(2)	*The Central Government may, by notification in the Official Gazette, appoint. Different dates may be appointed for enforcement of different provisions of the Draft Bill.*	**Clarity on the timeline of appointment of provisions will help entities prepare and adopt necessary measures to ensure compliance with the provisions as and when they are implemented.** a. The timeline for implementation of different provisions has not been specified. Since the provisions require entities to carry out modifications and/or adopt suitable measures to ensure compliance, lack of clarity may cause uncertainty amongst stakeholders. An indicative timeline (at least 6 months) for enforcement of the Draft Bill will help entities adopt necessary practical measures timely, and manage compliance costs.
Protection to Foreigner Personal Data – Section 18(1)(d)	*The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where: personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India*	**Certain protections may be made applicable to foreigner personal data processed in India as well.** a. Foreigner's personal data brought into India by an Indian entity pursuant to a contract with an overseas entity. As per Section 18, only certain provisions have been extended to such data; rights of data principals, mechanisms for cross-border data transfers, and protecting with appropriate safeguards. However, certain provision of the Draft Bill, such as notifying affected data principals, retaining data for legal requirements, etc., are not applicable to foreigner's personal data. For reference, certain overseas statutes require foreign entities to assess laws of third countries to determine if the personal data to be transferred shall be accorded "sufficient protection" in case of data access requests. The Hon'ble Supreme Court's rulings have also expressly held that foreigners are entitled to fundamental right to life provided under Article 21 of the Indian Constitution, 1950[17], which includes the right to privacy[18]. As such, it may be worth re-evaluating protections applicable to foreigner's personal data.

[17] In *Selvi & Ors.* v. *State of Karnataka* (AIR 2010 SC 1974), the Indian Supreme Court noted that Article 21 of the Indian Constitution has been given a 'non-derogable' status (i.e., it cannot be infringed under any circumstances) and is available to citizens as well as foreigners.
[18] In the case of *Justice K.S. Puttaswamy* v. *Union of India* (AIR 2017 SC 4161), confirmed that the Indian Constitution guarantees each individual the fundamental right to privacy.

We hope these comments are helpful. We are thankful for the opportunity to engage with the ministry in this consultation.

Please feel free to reach out to us for any assistance required in respect of the formulating the future legal framework of the digital ecosystem in India.

Prashant Daga, Advocate

BTG Legal Services
prashant.daga@btglegal.com