The Global Data Alliance[1] welcomes the opportunity to share its views on the Personal Data Protection Bill 2019 with the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019. The Alliance is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. Alliance companies rely on the ability to transfer data responsibly around the world to create jobs and make local industries more competitive. Cross-border data transfers power innovation and growth across the globe and all sectors of the economy — from manufacturing and farming to local start-ups and service providers. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output.

Global Data Alliance members share a deep and long-standing commitment to protecting personal data across technologies and business models, as they recognize that today's cross-border economy depends on the trust of consumers and the general public. The Alliance, therefore, supports policies that protect personal data while enabling data to move across borders.

Although some aspects of the Bill would lay a strong foundation for a robust personal data protection framework in India, requirements of the Bill impeding or restricting data flows would pose substantial challenges to companies that operate internationally. Those challenges fall not only on global companies like Global Data Alliance members, but also on small and medium-sized enterprises based in India that use technology to serve customers across national borders. These restrictions on data flows create barriers that are disproportionate to the objectives of the Bill, which is to protect the data of Indian citizens.

Restrictions on the cross-border transfer of personal data in the form of data localization requirements do not advance personal data protection goals and trigger unintended consequences. They disrupt companies' operations and make it costlier to provide services in India, even if that was not their intent, effectively depriving end-users in India from the benefits of an outward-looking personal data protection framework and putting them at an economic disadvantage vis-à-vis end-users located in other countries. . The Bill imposes data localization requirements for two types of data: critical personal data and sensitive personal data. We urge these requirements be reconsidered.

CRITICAL PERSONAL DATA

According to Clause 33 of the Bill, critical personal data may not be transferred outside India. The bill does not define critical personal data and rather allows the Central Government to designate categories of personal data as critical without specifying any criteria for such designation. The absence of any clear criteria for classification of "critical personal data" creates more uncertainty for businesses and negative

[1] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members include BSA members and American Express, Amgen, AT&T, Mastercard, Panasonic, United Airlines, Verizon, Visa, and WD-40 Company. BSA | The Software Alliance administers the Global Data Alliance.

consequences for commercial operations, R&D, and continued investment. In addition, each time the Central Government were to designate certain types of personal data as critical, companies would have to go through an additional process to separate the newly classified critical personal data from other types of data, which would be extremely costly and sometimes unfeasible. This would lead to additional costs and would severely impact the ease of doing business in India, which contradicts Prime Minister Modi's Digital India vision to promote innovation and investments in India.

The Bill appears to contemplate transfers of critical personal data only after case-by-case determinations are made by the Central Government. This creates considerable uncertainty for businesses across a range of industries, because they have little ability to know in advance if the data they handle is considered critical – yet they would be prohibited from transferring the data altogether if it is deemed critical.

We recommend against imposing this restriction.

SENSITIVE DATA

Sensitive personal data may be transferred outside India as long as a copy of the data is kept in the country, according to Clause 33 of the Bill. Sensitive personal data is defined broadly and, in many cases, could not be separated from other types of data. As a result, the practical effect of the Bill is that nearly all types of data may be required to be stored in India. This would severely disrupt operations of both data fiduciaries ("**DFs**") and data processors ("**DPs**"), including limiting services available to DFs[2]. Moreover, the Bill would allow the Government to add new categories of "sensitive personal data," increasing regulatory uncertainty for businesses.

This requirement does not increase personal data protection. Nor does the separate restriction prohibiting transferring sensitive personal data outside India for the purpose of processing. That restriction would only allow sensitive data to be transferred outside India when both: (1) explicit consent is given by the data principal and (2) the transfer is made based on other safeguards per Section 34 of the Bill. Requiring companies to meet both requirements before transferring data outside India is duplicative, costly, and deviates from international best practices without increasing data protection. For example, according to Article 49 of the EU's General Data Protection Regulation (GDPR), explicit consent alone is a basis for transferring data to other countries, regardless of whether those countries have received an adequacy designation. Other appropriate safeguards are also sufficient basis for transferring data abroad.

We urge two changes to these provisions. First, when sensitive personal data is transferred outside India the Bill should not require a copy of the data be kept in India. Second, consent should not be required when the transfer of data is based on a legal ground such as an adequacy decision or, in its absence, in appropriate safeguards such as corporate binding rule or standard contractual clauses.

We appreciate the opportunity to share these recommendations and we hope they will be helpful as the Committee considers amendments to the Bill that would create a robust personal data protection environment in India, while allowing responsible stewardship of data to continue benefiting the citizens of India and the Indian economy.

[2] For instance, a company that has employees based in India and has its payroll functions centralized in another country would need to meet duplicative and costly requirements to be able process its payroll as the bill classifies financial data as sensitive personal information. This could harm Indian employees as they might not receive optimal payroll services offered to employees in other countries.