Thursday, October 19, 2023

Shri. Rajeev Chandrashekar
Minister of State,
Ministry of Electronics and Information Technology,
Government of India

SUBJECT: BSA INPUTS ON THE TIMELINES FOR IMPLEMENTING RULES UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT 2023.

Dear Shri. Rajeev Chandrashekar,

On behalf of BSA | The Software Alliance (BSA), I congratulate you and the team at Ministry of Electronics and Information Technology (**MeitY)** for formulating and passing the Digital Personal Data Protection Act, 2023 (**DPDP Act**).[1] We thank you for the public consultation meeting on Wednesday, September 20. BSA appreciates this opportunity to share our recommendations on the timelines for implementing rules (**Rules**) under the DPDP Act.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create the business-to-business technologies that other companies use. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, and their business models do not depend on monetizing users' personal data.

Based on our experience of working on privacy legislation globally, we strongly recommend that the MeitY provide a clear and reasonable transition period for business to come into compliance with the Act. Individuals, businesses, and the Government will benefit more from an orderly transition designed to increase compliance with the Act than an abrupt transition that requires catch-up under threat of enforcement.

We make two broad recommendations:

1. **Transition timeline:** Rules implementing the DPDP Act should be finalized at least 12 months before they take effect, to ensure that companies have sufficient time to operationalize their requirements. For provisions of the DPDP Act that do not require rulemaking, companies should be given a clear transitional period of at least 2 years for implementation.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc..

Le-Meridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001

P (91 11) 4978 9066
W bsa.org

2. **Stakeholder Consultation:** Rules should be issued after robust stakeholder consultations.

We explain these recommendations below and provide examples that illustrate the need for an orderly and sufficient transition to compliance with the DPDP Act.

1. Transition timeline

We strongly recommend adopting a transition timeline that provides companies time to come into compliance with DPDP's new requirements. Specifically:

- For provisions of DPDP that require rulemaking, companies should be given 12 months to comply after a final Rule is published.

- For provisions of DPDP that do not require rulemaking, companies should have two years from enactment of the Act to comply with its requirements.

This transition period is important for companies to update their products and services to comply with the DPDP Act. Once the Rules are finalized and published, implementation is likely to require many companies to change aspects of their products, such as software architecture, data systems and processes. Here are examples of DPDP provisions that we anticipate may require companies to implement changes to their products and services to comply with the Act:

a) Grounds for processing data – "Certain Legitimate use

The DPDP Act recognizes a narrow set of purposes for which companies can process data. The Act relies heavily on individual Data Principals consenting to the processing of their personal data under Section 5. Section 7 recognizes that companies may also process personal data for "certain legitimate uses" recognized in the Act. However, the Act recognizes a significantly narrower set of uses than other global privacy laws including General Data Protection Regulation (**GDPR**).

The DPDP Act's narrow set of legitimate uses will create significant practical concerns for companies seeking to implement its requirements — even for global companies that already comply with GDPR. Under GPDR, companies may rely on the legitimate interest ground for processing for a range of activities, including to manage customer relationships; to provide, operate, maintain and improve products and services; to improve customer service; to conduct research or request consumer opinions; to detect, prevent, or otherwise address fraud, and to protect the rights, property or safety of the company, its affiliates, or its customers. Because the DPDP Act does not recognize legitimate interests as a basis for processing, if a company relies on legitimate interests under GDPR, it may be required to instead seek consent from a data subject under DPDP Act or understand if another ground for processing is available once the Rules are issued. The same is true for companies that rely on the GDPR's provision allowing processing for contractual necessity, which is also not recognized in the DPDP Act. Complying with the DPDP Act's provisions on consent and legitimate uses therefore requires both review by the company's legal team, to assess the potential to process data under the Act's narrow legitimate uses, and ultimately by the product team, which may have to design and implement new consent requests or other changes across the company's products.

If companies are ultimately required to seek consent from consumers for activities they currently do not, it will require them to design new consent requests across their products. These large-scale changes are a significant undertaking and will become even larger when companies are required to adopt multiple new consent requests across dozens or hundreds of products. Given that software companies rely on regular design cycles to update the design and coding of their software-based products, these changes will require sufficient time to implement. For example, software design cycles are generally set on intervals of six months, nine months, twelve months, or eighteen months. Although smaller updates may sometimes be deployed outside of these regular cycles, larger

changes are built into a company's products and services through these established processes. As a practical matter, these established processes ensure that companies build-in privacy requirements robustly across products and services. Allowing companies sufficient transition time to comply with the DPDP Act will promote the use of these established processes, better serving the Act's goal of promoting privacy.

To the extent the Government of India used the DPDP Act's broad reservation of rulemaking authority to align the Act's approach to legitimate uses with the broader set of grounds for processing recognized under leading global privacy laws like GDPR (i.e., by expressly permitting processing based on legitimate interests and processing necessary for the performance of a contract), that approach would meaningfully ease the transition to DPDP for companies.

b) Notice

The DPDP Act specifically calls for new Rules for notices to be given when seeking consent from Data Principals. These notices will be particularly important, because companies may increasingly rely on notice and consent requests to comply with the DPDP Act given the narrow grounds for processing data for other purposes. This further heightens the need for specificity in rulemaking for notices under Sec. 5(1) and 5(2) (also refer Sec. 40(2)(a), (b)). These Rules on notices are also intertwined with the Act's provisions on legitimate uses, because they will establish the "specified purpose" for which personal data can be processed under Sec. 7(a), which is defined in Sec. 2(za).

Obligations under Section 5 cannot take effect until the abovementioned Rules set out the manner for notices to be issued to Data Principals. Until those Rules are in place, companies do not have enough guidance to create notices that are consistent with the Act.

Once Rules are finalized, companies can begin the process of designing new notices. However, updating notices to consumers is a time-consuming process for many companies. It requires them to re-architect consent requests and consumer-facing disclosures. It is also not practical for companies to implement a new set of consumer notices now and a second set once Rules have been issued. Thus, companies can coordinate the necessary changes between privacy, engineering, design, policy and legals teams only after the Rules are finalized and they identify the changes needed.

The time required to fulfil these obligations will be increased by the requirement created under Sec. 5(3) that every request for consent shall be presented in a clear and plain language, giving [the Data Principal] the option to access such request in English or any language specified in the Eighth Schedule to the Constitution. While this is important to make technology more accessible it also means that translating notices into all of the required languages will take a significant amount of time. Allowing for additional time will help ensure that all translations account for various ambiguities and nuances across different languages.

c) Reporting of data breaches

With respect to data breach obligations, companies are subject to several existing requirements — with differing timelines and reporting formats — to report breaches to sectoral regulators and the CERT-In. While it is important to comply with all these regulations to ensure security of different types of data, the incompatibility of different rules often can be confusing to companies. A new reporting format and timeline will require companies to develop new processes to ensure they are able to comply with the number of reporting requirements, which are different in nature but apply together.

The forthcoming Rules are to create a wide range of requirements for data breaches, including the form and manner for notifying both the Data Protection Board and individual Data Principals. Because the DPDP Act does not contain these needed details, no obligation to notify should take effect before at least 12 months after the Rules are promulgated to provide companies with sufficient time to implement their obligations.

In addition, the DPDP Act does not set a clear threshold to identify the set of data breaches that require notification to the DPB or to Data Principals. To the extent that implementing Rules set such a threshold, it would ease the ability of companies to implement these new requirements more quickly. For example, a breach of personal data that is unusable, unreadable or indecipherable to an unauthorized third party due to use of methods such as encryption, redaction, access controls, or other mechanisms should not trigger notification requirements. We recommend the Rules create a risk-based threshold for reporting data breaches and only require notification for breaches that create a significant risk of material harm to Data Principals.

d) Other areas of rulemaking

- **Significant Data Fiduciaries (SDFs):** Under Sec. 10, the Government is to notify a Data Fiduciary or class of Data Fiduciaries that they are an SDF. The process of notifying SDFs is still uncertain. SDFs are to: (1) appoint a data protection officer, (2) appoint an independent data auditor, and (3) undertake compliance measures including a periodic Data Protection Impact Assessment (DPIA), periodic audit, and other measures to be prescribed under Sec. 40(2)(k) and 40(2)(l). Given the uncertainty and heightened obligations, **SDF obligations should not apply until at least one year after company is notified it is SDF. In addition, these obligations should apply no sooner than one year after the Rules on SDF obligations are finalized.**

- **Data Principal rights requests:** Under Sec. 11(1), 12(3), 11(1)(c), and Sec. 12(3), the forthcoming Rules are to establish the manner of exercising rights requests. Because Rules must set out the manner for Data Principals to exercise their rights, the obligation to honor rights requests should not take effect 12 months until after those Rules are published. Substantively, if the forthcoming Rules align the DPDP's requirements for rights requests with the GDPR's requirements for rights requests, the timeline to implement these obligations would be less concerning.

  Currently, our concerns with these rights requests are:

  i. Under Section 11(1)(b), the Data Principals have a right to "the identities of all other data fiduciaries and data processors with whom personal data is shared". This would require companies to provide additional information than is required under GDPR, which only requires disclosure of the "categories" of recipients, not specific company names. In addition, the specific identity of every single Data Processor is likely of somewhat limited value to Data Principals since Data Fiduciaries are responsible for any processing carried out by Processors under existing laws (including under Sec. 8(1) of the Act). The requirement to disclose the identities of Data Processors generally is a significant difference from other global data privacy regimes.

  ii. The Act does not state how long companies have to respond to a request. We recommend that implementing Rules specify that companies have one month to respond, with the possibility of extension by an additional two months, in line with GDPR Art. 12(3).

  iii. The Act does not include standard exceptions to these rights that recognize companies do not have to respond to rights requests that create cybersecurity risks, or when a correction request seeks to correct data that is not inaccurate, or to erase data that is needed for compliance with a legal obligation. We strongly recommend the forthcoming Rules recognize such exceptions.

- **Data retention:** Data retention obligations require detailed rulemaking because the Act's obligation is to delete data if the data principal does not approach the data fiduciary within a

time period to be set by the Rules. Under Sec. 8(8), the forthcoming Rules may create different retention periods for different classes of data fiduciaries and for different purposes. To implement these requirements, companies will need to know the specific retention time period. We therefore recommend these obligations take effect no sooner than one year after Rules are final.

2. Stakeholder Consultation

The forthcoming Rules should be developed through a robust and meaningful stakeholder engagement process that provides the time and opportunity for all interested parties to contribute to achieving the goals of the Act. This includes establishing and communicating clear timelines and milestones for public consultation, consulting extensively on draft rules with key stakeholders, including private sector entities, and allowing sufficient time for robust engagement with stakeholders. Clearly communicating the timelines and milestones for the public consultation process would assist stakeholders in understanding when implementing rules of the Act will be published and the expected timeframe for subsequent implementation. Such clarity would contribute to an efficient and transparent regulatory process in which stakeholders can examine draft rules in depth and provide meaningful feedback on specific recommendations. Comprehensive and robust engagement of stakeholders will help the government achieve its regulatory goals. This will allow all affected stakeholders to contribute to the law-making process at every step and ensure that the government remains accountable when implementing the Act.

* * *

Thank you for your continued leadership and commitment to safeguarding privacy and enhancing trust in the digital ecosystem. We welcome an opportunity to further engage with your office on these important issues.

Please do not hesitate to contact the undersigned at venkateshk@bsa.org if you have any questions or comments regarding our suggestions.

Sincerely,

Venkatesh Krishnamoorthy
Country Manager - India