REQUEST FOR COMMENT RESPONSE

DIGITAL PERSONAL DATA PROTECTION BILL

December 17, 2022

I. INTRODUCTION

In response to the Ministry of Electronics and Information Technology's ("MeitY") request for feedback on the proposed Digital Personal Data Protection Bill 2022 ("DPDP Bill") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international cybersecurity provider that defends globally distributed enterprises from globally distributed threats. We directly support organizations of all sizes, public and private, in India and help them identify, prevent, and defend themselves against cyber threats. CrowdStrike also is proud to have a talented workforce based in India.

CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in responding to and protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

MeitY has written a thoughtful draft legislation with the goal of improving data protection and security. While we do not have feedback on every aspect, we do want to offer several points that may be of value to the Ministry as it continues to develop the bill.

A. *Scope*

We note that the DPDP Bill does not apply to non-personal information and only applies to digital information. Similar to other data protection approaches around

the globe, this reflects a practical focus on protecting data related to individuals without mischaracterizing all data as having the same privacy equities nor stifling the use of data for technological innovation. For example, analysis of security telemetry data, such as machine events, at scale is fundamental to protecting against personal data breaches.

To achieve true data protection, both personal and non-personal information are used to identify and stop security attacks[1], and understanding the scope of the DPDP Bill's proposed requirements better ensures that privacy and security practitioners can design their compliance programs accordingly. Accordingly, it is important not only to draw this distinction but also to ensure that personal data can be processed for legitimate means. For example, cybersecurity best practices, such as identity protection, endpoint detection and response, log management, and threat hunting are dependent upon unique identifiers, which may incidentally be categorized as personal information, to detect and mitigate security risks. This includes identifying which assets are being targeted by an adversary, whether or not a threat actor has moved laterally across a network, and mitigating the impact of breach attempts. In other words, a defender would not know which accounts had been targeted, when privileges were escalated or what data was exfiltrated if the processing of identifiable information were not permitted. We recommend any further versions of this Bill continue to only apply to personal information and follow the lead of other global data protection laws in permitting the processing of personal data for data protection and cybersecurity.

B. Cross Border Data Transfer

Notably, the DPDP Bill does not include an explicit data localization clause. However, the inclusion of clauses limiting cross border data transfers can effectively create the same unintended consequences of data localization, even if that is not the intent of such clauses. Under the Bill, the central government will "notify" as to which countries data can be transferred, implying that data cannot be transferred outside India without government approval. CrowdStrike recommends MeitY provide additional information or continue stakeholder engagement and ask

[1] *Data Protection Day: Harnessing the Power of Big Data Protection* https://www.crowdstrike.com/blog/data-protection-day-cybersecurity-best-practices/

for feedback about what criteria a country must meet and what the process for such notification from the government entails.

Further, the DPDP Bill does not include other transfer mechanisms options, such as standard contractual clauses (SCC) or binding corporate rules. In order to remain future-flexible, it is important to prioritize the goal of protecting data regardless of where it is, rather than equating data protection with restrictions on cross border data transfers. Consequently, providing as many means as possible to lawfully transfer data abroad will continue to afford Indian organizations the ability to create and use innovative technologies on a global scale.

Today, India plays an important role contributing robust technical talent and IT infrastructure to global organizations. This invariably involves cross-border data flows, whether it is to maintain IT system authentication or as part of ensuring unified security visibility. Consequently, rigorous restrictions on where data may be transferred, with an approved country list, might have the effect of limiting innovation and the technological offerings available in India. If the pre-approved country approach is maintained in the DPDP Bill then it is critical to clarify the countries to which data transfer will be permitted, along with the criteria for making those decisions. We recognize that the ultimate purpose of data protection laws is to protect data subjects' rights and interests; however, any actions that in effect create data localization will limit defenders' means to identify, detect and respond to data breaches without restricting adversary behavior. Put simply, data localization is not a proxy for data protection. Instead, data protection requires a holistic approach to protecting both privacy and security. Cyber threat actors will transfer breached data out of India regardless of whether or not transfer rules are in place. Accordingly, amending the DPDP Bill language to include additional transfer mechanisms, such as SCCs or binding corporate rules, would play a large part in ensuring the best technologies, SaaS solutions, and 24/7 coverage can continue to be used to protect personal data against data breaches.

C. Data Breach Notification

According to the DPDP Bill, every data breach should be reported to the Data Protection Board (DPB) regardless of the magnitude of the risk. However, to avoid imposing unreasonable burdens on data fiduciaries and data processors, the types

of data breaches that fall under the reporting regime should be limited to only breaches that could cause significant harm to data subjects. Additionally, the DPDP Bill requires data fiduciaries and processors to notify data subjects of a breach - no matter the size – which is not viewed as a best practice from CrowdStrike's security perspective.

Mass breach notifications would adversely affect the cybersecurity and privacy interests that the DPDP Bill seeks to protect. This is because mass breach notifications risk publicly revealing the digital supply chain of affected parties. Revealing such information to a broad group of data subjects makes it likely that a bad actor or adversary can leverage such information to engage in cybercrime or threatening cyber behavior, such as supply chain attacks and targeted phishing schemes. As a leading cybersecurity provider, it is our view that perhaps the most significant threat to personal data comes from threat actors operating unlawfully. While responsible data controllers and processors adhere to robust compliance programs, cyber adversaries do not play by the rules.

Any mandatory data breach reporting should be predicated upon a risk and impact driven approach. For example, many global data breach reporting obligations only require breach reporting where there is a risk of harm to affected individuals. Another important distinction that merits discussion is that of risk versus high risk. Not all breaches have the same level of severity. For example, an incident where a threat actor sees a list of user names might have a small or negligible impact on affected parties. Whereas, another incident in which a threat actor exfiltrates complete financial or medical records may have a severe impact.

Focused data breach reporting obligations that are easy to follow and organize around can help incentivize organizations, including government agencies, to adopt adequate technical and organizational cybersecurity practices. Requiring reporting for all breaches does not create an incentive structure or raise security.

Finally, as a practical matter a data controller rather than a data processor is generally the best suited to determine whether or not a breach has occurred, the nature of the risk posed to data subjects, and how to contact individuals. Indeed, a data processor often does not have the full picture of how a breach on their infrastructure may affect a controller's data nor know how to contact data subjects

in the event of a breach. CrowdStrike recommends that the DPDP Bill be amended to require data processors to report to data fiduciaries instead of directly reporting to DPB or data subjects.

III. CONCLUSION

MeitY's proposed DPDP Bill provides a thoughtful analysis of a complex legal and policy area. As updates to the law and administrative rulemaking moves forward, we recommend continued engagement with stakeholders. There is a unique opportunity to raise the bar on data protection in India, and it is critical to recognize that cyber threats pose some of the greatest risks to privacy today. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***