REQUEST FOR COMMENT RESPONSE

The Implementing Regulations of the Personal Data Protection Law in the Kingdom of Saudi Arabia

July 31, 2023

I. INTRODUCTION

In response to the Saudi Data and Artificial Intelligence Authority's ("SDAIA") request for feedback on the *Implementing Regulations of the Personal Data Protection Law* ("PDPL Implementing Regulations"), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. 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 protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We commend the incorporation of common global privacy principles and risk-based security requirements into the amended draft of the PDPL Implementing Regulations. CrowdStrike submitted comments to the SDAIA in March 2022,[1] and we are pleased to see some of our suggestions make their way into the newer iterations of the Implementing Regulations, as well as into the new draft Regulation on Personal Data Transfer outside the Geographical Boundaries of the Kingdom, which we are commenting on separately. While we do not have feedback on every aspect of the proposed PDPL Implementing Regulations, we do want to offer several points that may be of value to the SDAIA on its journey to a comprehensive national personal data protection regulation.

Article 1. Definitions

[1] *"Kingdom of Saudi Arabia Data & Artificial Intelligence Authority: Draft of the Executive Regulation of Personal Data Protection Law (PDPL),"* CrowdStrike, March 25, 2022. https://www.crowdstrike.com/wp-content/uploads/2023/02/2022_03_25_KSA-PDPL.pdf

Article 1 defines a personal data breach as "any incident that leads to unauthorized disclosure, destruction, or access to personal data, whether intentional or accidental, and by any means, whether automated or manual."

Using this definition for the various requirements (such as reporting and notification requirements) listed in the document risks a volume of reporting that is so great it creates "noise" for the SDAIA and extra work for those impacted by a low-impact threat activity. Therefore, in defining what constitutes a data breach and level of harm, it is critical to focus on internationally-accepted principles-based concepts rather than prescriptive technical requirements. CrowdStrike recommends adopting a risk-based approach and take the following factors into consideration:

- Nature of the data in question: Could the data in question be used by a threat actor to cause significant harm to individuals?
- Impact of a breach: Was the data successfully exfiltrated and, if so, to whom was the data exfiltrated?
- Mitigations: Did the carrier successfully mitigate impacts?

CrowdStrike recommends clarifying what an "eligible breach" is and considering the following distinctions to narrow the scope of the definition of "eligible breach."

Alerts versus Incidents. In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and standards. In most cases, carriers using contemporary cybersecurity solutions should be alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or the compromise of a single account. In most scenarios where defenders see these alerts and address them quickly, an issue does not meet any reasonable standard of a cybersecurity "incident" because the threat actor has not meaningfully achieved their objective or accessed sensitive information. With this in mind, an alert should not be included in the definition of "breach."

Impact versus Serious Impact. Another important distinction that merits discussion is that of impacts versus serious impacts. 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. Consideration of the impact and severity of a breach is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures.

Mitigated Attacks. Threat actors may choose to target an organization in a series of steps, rather than in a single attack. In fact, an initial intrusion into an enterprise is often not a threat actor's end goal. Instead, threat actors may first deploy a backdoor, harvest credentials, or use other methods in order to move laterally throughout a network and to their ultimate objective. A threat actor may be stopped at any of the steps in the killchain, and this raises important questions that impact the breach notification process - namely, if a breach is mitigated, does the obligation to notify still exist? For example, if a threat actor enters an enterprise with the goal of exfiltrating data but is stopped before the infiltration occurs, the possible resulting impact of the incident has been mitigated. In such an example, it is a breach when the threat actor enters the network but it could have been a substantial breach if the goal of data exfiltration was reached. Ultimately, this means that a data breach in and of itself may not pose a risk of harm to consumers where successful steps have been taken to mitigate the breach and prevent exfiltration. Mitigated breaches should not be included in the reporting scope.

Article 24. Information Security

Article 24 of the PDPL Implementing Regulations says "The Controller shall take the necessary organizational, administrative, and technical measures to ensure the privacy of the Data Subject and the security of Personal Data, and shall comply with the following: a) Implement appropriate security and technical measures to limit security risks related to Personal Data; b) Comply with relevant controls, standards, and rules issued by the National Cybersecurity Authority or recognized best practices and cybersecurity standards if the Controller is of a special nature."

We applaud the emphasis on appropriate security and technical measures, as well as cybersecurity standards and best practices. To accomplish these objectives, we recommend this article specify certain security and technical measures that organizations can adopt. We suggest the following cyber best practices, many of which would complement the Kingdom's Cloud Cybersecurity Controls (CCC 2020) regulation[2]:

- **Cloud Services**. Leveraging cloud systems provides a series of potential security enhancements. Retiring legacy applications and infrastructure reduces attack surface and points of failure. Cloud systems enable comprehensive visibility of workloads. For security technologies specifically, native cloud-based solutions provide robust and scalable protection of distributed environments.

[2] "*Cloud Cybersecurity Controls* (CCC - 1 : 2020)," Kingdom of Saudi Arabia National Cybersecurity Authority, https://nca.gov.sa/ccc-en.pdf, page 21, notes the requirement to implement "modern technologies, such as Endpoint Detection and Response (EDR)".

- **Extended Detection & Response (XDR).** The next evolution of the ***Endpoint Detection and Response (EDR)*** concept, XDR seeks to leverage rich endpoint telemetry and other security-relevant data, wherever it exists within the enterprise. EDR is a natural baseline security capability, but XDR drives more comprehensive cybersecurity outcomes.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. Machine learning (ML) and artificial intelligence (AI) are essential to meeting constantly-evolving threats.

- **Identity Threat Protection**: As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, cloud services multiply, and enterprise boundaries continue to erode. This trend increases the risk of relying on traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and ML analytics to quickly identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

- **Speed**. When responding to a security incident or event, every second counts. The more defenders can do to detect adversaries at the outset of an attack, the better the chances of preventing them from achieving their objectives. Adversaries work rapidly at the outset of breach to move laterally and escalate privileges, seeking to gain access to more systems and data and ensure persistence. This means that organizations should measure and reduce their response time.[3]

- **Threat Hunting**. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, properly trained and resourced defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The better-instrumented the environment, the more chances defenders give themselves to identify malicious activity as an attack progresses through phases. Multiple opportunities for detection increase defenders' chances of success and help avert "silent failures."

[3] Elite organizations seek to identify a breach attempt within one minute, investigate within ten minutes, and isolate or remediate threats within sixty minutes.

- **Zero Trust Architecture.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Service Providers**. Some entities lack the cybersecurity maturity to run robust security programs internally, or seek to apply internal IT/security resources toward domain-specific challenges. Increasingly, such entities should rely upon managed security service providers to strengthen their security posture.

Article 25: Notification of Personal Data Breach

CrowdStrike is pleased to see the SDAIA adopting the emerging best practice of a notification time frame of 72 hours, which we recommended in our earlier comments.[4] However, please see our response to Article 1 on the definition of a data breach. We recommend that any reporting timeline requirements be considered in context. As discussed in our response to Article 1, not all cyber incidents have the same level of severity and rise to a level of individual harm that necessitates reporting or notification. We recommend the SDAIA limit the reporting requirement to focus on unauthorized access that would potentially cause catastrophic or systemic impacts.

Article 33: Transfer or Disclosure of Data to Entity outside the Kingdom

CrowdStrike has submitted a separate comment on the "Regulation on Personal Data Transfer outside the Geographical Boundaries of the Kingdom," but we want to provide a brief summary of our main points here as well, given that the draft Data Transfer Regulation is part of the PDPL Implementing Regulations.

Article 29 of the amended PDPL, and Article 33 of the PDPL Implementing Regulations pertain to the "Transfer or Disclosure of Data to Entities outside the Kingdom." Both of these texts contain references to data transfers that "serve the interests of the Kingdom," as well as noting that "the transfer or disclosure shall not prejudice national security or the

[4] *"Kingdom of Saudi Arabia Data & Artificial Intelligence Authority: Draft of the Executive Regulation of Personal Data Protection Law (PDPL)*," CrowdStrike, March 25, 2022. https://www.crowdstrike.com/wp-content/uploads/2023/02/2022_03_25_KSA-PDPL.pdf

vital interests of the Kingdom." As a leading cybersecurity provider, it is our view that the greatest threat to data comes not from data transfers, but from cyberattacks with potentially disastrous consequences, including for national security. Therefore, in considering certain restrictions of data transfers in the name of national security, we urge the SDAIA to consider the following.

It is important to incentivize strong technical mechanisms for data protection, rather than focusing on data sovereignty, which cyber threat actors ignore. Adversaries transfer data across borders in data breaches, while defenders comply with the law. The most significant threat to data and national security today come from such threat actors operating unlawfully. Therefore, national laws should focus on stopping data exfiltration by bad actors rather than localization requirements that will not be followed by adversaries.

The proposed limitations on data transfers outside the Kingdom in the name of national security or to protect the interests of the Kingdom, can actually end up lowering cybersecurity capabilities which leads to a decreased ability to protect data, and threaten the Kingdom's ability to manage cybersecurity risk.[5] Research has shown that limiting data transfers can have an adverse impact to cybersecurity and restricts the ability of defenders to follow best practices.[6] Data sharing limitations reduce the ability of countries to identify, protect, detect, respond, and recover in the face of cyberattacks.

The Kingdom's Cloud Cybersecurity Controls (CCC 2020) document rightfully creates an exception for cybersecurity data, reflecting the realities of Saudi Arabian companies' enterprise-wide needs. Specifically, article 2-3-P-1-12 of that document requires covered entities to implement "modern technologies, such as Endpoint Detection and Response (EDR) technologies (such as CrowdStrike's Falcon Platform), to ensure that the information servers and devices of cloud service providers (CSPs) are ready for rapid response to incidents."[7] Consistent with this regulation, we suggest a focus on strong technical controls (the cyber best practices discussed above) rather than on data sovereignty.

III. CONCLUSION

The SDAIA's proposed regulations provide a thoughtful analysis of a complex legal and policy area. As updates to the Implementing Regulations of the PDPL move forward, we recommend continued engagement with stakeholders. Finally, because the underlying

[5] *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures*, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466479.
[6] *Ibid.*
[7] "*Cloud Cybersecurity Controls (CCC - 1 : 2020)*," Kingdom of Saudi Arabia National Cybersecurity Authority, https://nca.gov.sa/ccc-en.pdf, page 21

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®, 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/.

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

Rob Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***