REQUEST FOR COMMENT RESPONSE

Regulation on Personal Data Transfer outside the Geographical Boundaries of 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 *Regulation on Personal Data Transfer outside the Geographical Boundaries of the Kingdom* ("Data Transfer Regulation"), 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

CrowdStrike welcomes the incorporation of common global privacy principles and the emphasis on risk-based security requirements into the new draft Data Transfer Regulation. CrowdStrike provided comments to the SDAIA's Draft Implementing Regulations of the Personal Data Protection Law (PDPL) in March 2022, which included commentary on this topic, and we are pleased to see several of our recommendations incorporated.[1] We have studied the draft Data Transfer Regulation and how it fits into the new draft PDPL Implementing Regulations, which we will be commenting on separately. In this comment, CrowdStrike offers ideas to further improve key data protection equities as the SDAIA considers how to evaluate levels of data protection, exemption cases, risks, as well as safeguards for transferring personal data outside the Kingdom. Our comments will start by focusing on Article 9 (risk assessment), as this will provide the context for our comments on Article 6 (safeguards).

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

Article 9. Risk Assessment of Transferring or Disclosing Data outside the Kingdom

Article 29 of the amended PDPL, and Article 33 of the Draft 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 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.[2] Research has shown that limiting data transfers can have an adverse impact to cybersecurity and restricts the ability of defenders to follow best practices.[3] Data sharing limitations reduce the ability of countries to identify, protect, detect, respond, and recover in the face of cyberattacks.

We recognize the problem that the SDAIA is trying to address, but hope that these well-intentioned efforts will not hurt productive uses of data transfers like cybersecurity. CrowdStrike consistently warns against such cases of data localization as a misplaced proxy for cybersecurity. A few examples of these include France's draft cybersecurity certification, SecNumCloud,[4] an early draft of Italy's Presidential Decree implementing NIS 1.0,[5] certain interpretations of post-Schrems II cross-border data flows, and other policies

[2] *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures*, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466479.

[3] *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures*, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4466479

[4] *Cloud Computing Service Providers (SecNumCloud) Requirements*, 2022. https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf

[5] *Regulation on notifications of incidents having an impact on networks, information systems and information services*, 2019.

promoting data sovereignty for domestic intelligence gathering and industrial policy objectives, which ultimately end up being detrimental to cybersecurity.[6]

Article 6. Safeguards for Transferring Personal Data outside the Kingdom

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 that covered entities 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 the Kingdom's CCC regulation, we suggest a focus on strong technical mechanisms. Data protection is best achieved where international transfers of personal data are permitted with practical safeguards, as well as the adoption of best-in-class technologies and service providers. Therefore, to complement the CCC's high standards, we suggest that the SDAIA incentivize best practices of cybersecurity given the risks from data breaches. We recommend the following cyber best practices:

- **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.

- **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 and artificial intelligence are essential to this

https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg

[6] *Data Protection Day 2023: Misaligned Policy Priorities Complicate Data Protection Compliance*, 2023. https://www.crowdstrike.com/blog/data-protection-day-2023-misaligned-policy-priorities-complicate-data-protection-compliance/

[7] "*Cloud Cybersecurity Controls* (CCC - 1 : 2020)," Kingdom of Saudi Arabia National Cybersecurity Authority, https://nca.gov.sa/ccc-en.pdf, page 21

end. Leveraging these technologies is 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 upon 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 machine learning 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.[8]

- **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."

- **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.

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

- **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.

III. CONCLUSION

The SDAIA's proposed laws provide a thoughtful analysis of a complex legal and policy area. 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 and data portability. Consequently, providing as many means as possible to lawfully transfer data abroad will continue to afford Kingdom-based organizations the ability to create and use innovative technologies, including data security and privacy technologies, on a global scale. As updates to the Data Transfer Regulation move forward, we recommend continued engagement with stakeholders. 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®, 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 and Strategy

Email: policy@crowdstrike.com

***