CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Kingdom of Saudi Arabia Data & Artificial Intelligence Authority: Draft of the Executive Regulation of Personal Data Protection Law (PDPL)

March 25, 2022

I. INTRODUCTION

In response to the Kingdom's Data & Artificial Intelligence Authority's Draft Regulations to the PDPL, CrowdStrike appreciates the opportunity to offer the following views. CrowdStrike approaches the request for comments 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 commends the incorporation of common global privacy principles and security best practices into the draft PDPL. Cyber attacks from advanced nation-state actors, criminal groups, and hacktivists pose a substantial threat to the safety of personal and other sensitive data. Accordingly, this response highlights areas where CrowdStrike offers ideas to further improve key data protection equities.

A. Emerging Technologies

The draft law mentions emerging technology and specifically references artificial intelligence. Our comments will focus on the use of AI/ML within cybersecurity solutions. Legacy cybersecurity solutions used to rely on scanning files against signatures of previously identified malicious files. This process was onerous, resource-intensive, and could be easily circumvented through the use of novel or

slightly modified approaches. Next-generation solutions, which leverage AI/ML, can detect previously unknown threats based on their characteristics or behaviors. This offers much more robust protection against threat activity.

Leveraging AI/ML can achieve success against unknown unknowns. For example, a machine learning model, shipped to CrowdStrike's Falcon Platform customers in September 2019, detected with high confidence the SUNSPOT malware, which was central to a sophisticated campaign that targeted high-value government organizations in late 2020-early 2021.[1] This is one of many instances of AI/ML typifying the best ways to defeat threat actors using new or tailored tools, tactics, techniques, or procedures.

In cybersecurity, AI is an advantage, especially when added to enterprise security solutions.[2] Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. Indeed, with the help of AI, CrowdStrike can stop an attack in its tracks because such technology works faster than conventional signature-based or indicator of compromise (IOC)-based prevention.

We understand that a concern with AI is the possible harm to individuals, but for AI, like for any other technology, the context in which it is used, rather than the mere fact that it is incorporated, is material. Consequently, relying upon a right to object to a particular technology or data processing methodology is not the best approach to protect rights in an ever-evolving technological landscape.

We recommend that as the PDPL is further developed, flexibility is kept in mind. By this, we mean to emphasize the flexibility of AI as a positive tool in various

---

[1] Sven Krasser, "Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware," CrowdStrike Blog (Jan. 21, 2021) https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/.

[2] Michael Sentonas, *How Artificial Intelligence is Becoming a Key Weapon in the Cybersecurity War*, CrowdStrike Blog, Oct. 24, 2017, https://www.crowdstrike.com/blog/how-artificial-intelligence-is-becoming-a-key-weapon-in-the-cybersecurity-war/.

situations, and not simply an automated-decision making system that could harm individuals. We further recommend protecting the rights of citizens through a technology-neutral approach. When creating regulations on the safe use of AI, the Data & Artificial Intelligence Authority should consider adopting language similar to the GDPR's requirement that organizations implement safeguards "appropriate" to the risk to protect personal information. This approach incentivizes organizations to take into account modern, rapidly-evolving data breach risks posed by cybersecurity threats from e-crime, 'hacktivist', and nation state actors using tactics such as ransomware, supply chain attacks, or malware-less intrusions.

B. Security and Incident Response

With regard to breach notification, we recommend that the Data & Artificial Intelligence Authority consider adopting a longer time frame of 72 hours or a common standard like "as soon as practicable" in lieu of the currently-proposed "immediately" requirement. Organizations often need to rely upon outside support from law firms and cybersecurity service providers to gather enough information for even initial incident reporting. An "immediate" notification requirement may not yield meaningful information about an incident. Consequently, notifications that simply indicate something going wrong is equally problematic because it will create additional "noise," making it much more difficult for security professionals and regulators to prioritize. In fact, where the notification is prioritized in too short a timeframe, it may drain resources from focusing on mitigating the incident and may lead to inaccurate information being passed to potentially affected users or a false sense of security for those not determined to have been impacted at that stage.

C. Implementation of Appropriate Technical and Organizational Measures

We applaud the emphasis on risk-based security requirements in the draft PDPL. Threats evolve and security must too. CrowdStrike believes that breaches can be prevented by ensuring that appropriate organizational, physical and technological security measures have been taken. For example, it is vital for organizations to incorporate new security measures that put an emphasis on authentication, such as Zero Trust. Zero Trust requires users to reauthenticate or re-establish permission for whichever device or resource they want access to, as opposed to authenticating

once on a device and automatically having access to all the resources therein.[3] This holistic view of authorized identity helps to reduce or prevent lateral movement and privilege escalation during a security incident or event.

There is often a misconception that breaches can only be stopped through proper patch management and by the use of appropriate anti-malware detection systems. In reality, cybersecurity threats are exceptionally broad and niche solutions can be too narrow. The full scope of a problem will not be resolved by a box on a network or a single-purpose software agent. Effective breach prevention requires contextual awareness and visibility across environments, including within cloud and ephemeral environments.

Many data breaches take place without the use of malware, leveraging instead harvested credentials, misconfigured account services, native or legitimate administration tools, or supply chain attacks.[4] Accordingly, appropriate security measures must include more than anti-malware detection systems and patch management. For example, the Executive Order on Improving the Nation's Cybersecurity[5] calls for the implementation of Endpoint Detection and Response (EDR), whereas the European Union Agency for Cybersecurity (ENISA) advises in its "State of the Art" guide that extended detection and response (XDR) solutions should be considered to protect against breaches.[6] XDR seeks to apply order to a sometimes chaotic array of security tools by deriving actionable insights wherever they exist within the enterprise, such as from EDR data, authentication logs, and network telemetry.

D. Cross-Border Data Flows

Today's economy and its success depends more than ever before on cross-border data flows and data portability. This trend will continue, especially in light of the

---

[3] CrowdStrike's Threat Report 2021, https://www.crowdstrike.com/global-threat-report.
[4] CrowdStrike's Threat Report 2021, https://www.crowdstrike.com/global-threat-report.
[5] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; *See also* New Cybersecurity Executive Order: What It Means for the Public Sector, https://www.crowdstrike.com/blog/what-the-new-cybersecurity-executive-order-means-for-public-sector/
[6] IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the Art" Technical and Organizational Measures, Teletrust (2021), https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Guideline_State_of_the_art_in_IT_security_EN.pdf.

digital transformation accelerated by Covid-19 and the "work from anywhere" movement, as well as the need for improved collaboration capability among the international operating workforce. Accordingly, it is important to incentivize organizations in the Kingdom to adopt the best technologies and third-party service providers for their use cases. Rigid cross border data flow restrictions can significantly limit choice.

In the few jurisdictions where rigid data residency or localization requirements exist, they may inadvertently inhibit data protection without offering clear benefits to privacy. In fact, data residency or localization requirements can reduce the level of data protection by limiting the application of state of the art technology and safeguards, in the event they are unavailable in the country of origin, or require outsourcing and cross-border data flows.

Also, the importance of cross-border data flows is far-reaching, and affects individuals, entities, and society more broadly. Any restriction on cross-border data flow or data portability requirements could have adverse implications for the Kingdom's innovation, jobs, and access to services. This means that it is critical to provide organizations with deference to make their own context-informed and critically, risk-informed–decisions about cross-border data by adhering to core data protection principles related to the circumstances of specific transfers.

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.

Further, cross-border data flows and unrestricted data portability are necessary elements of some of today's most sophisticated cybersecurity solutions. Many of the most innovative technologies for protecting personal data against data breaches leverage global endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and cross correlation of indicators of attack. Moreover, modern IT infrastructure in general invariably involves cross-border data transfers.

Data protection is best achieved where intentional transfers of personal data are permitted with practical safeguards, while unintentional transfers of personal data via data breaches are thwarted by protecting against ever-evolving cybersecurity threats with innovative technologies. 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.

As a consequence, we recommend amending Article 28 et seq. of the draft PDPL to better enable cross-border data flows and incentivize adoption of best-in-class technologies and service providers.

This includes modifying the current proposed Controller obligation to obtain prior written approval on a case-by-case basis from the competent regulatory authority. Although well-intended, this may stifle the ability of organizations to adopt best-in-class technologies and services, and it deviates from global data protection policy trends. By way of example, the European Union (EU) intentionally moved away from a prior authorization model in favor of GDPR's stakeholder responsibility approach. EU policy makers determined that such requirements had been too cumbersome, laborious, bureaucratic and slowed down the economy and sometimes even innovation. We consider the GDPR cross-border data transfer requirements (Art. 44 et seq.) as appropriate to protect personal data, safeguard privacy, maintain an adequate level of data protection at transfer, and provide useful beneficiary rights to individuals.

As to the requirement of conducting an impact assessment, we would appreciate better clarification and information to the content, format, and scope of the required 'impact assessment'. With respect to other jurisdictions' privacy impact regulations, we experienced guidance to impact assessments as a great benefit.

III. CONCLUSION

The PDPL draft incorporates a thoughtful analysis of a complex legal and policy area, demonstrating the Kingdom's commitment to data protection. As PDPL is further developed, we recommend continued engagement with international

stakeholders. Adversaries innovate at a record-pace, and it's important to empower defenders to leverage global data flows, big data analytics, and machine learning to protect against ever-evolving threats. Finally, because the underlying technologies evolve faster than law and policy, we emphasize the importance of principles-based framework rather than prescriptive requirements.

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

Dr. Christoph Bausewein CIPP/E
Director & Counsel, Data Protection & Policy

Email: policy@crowdstrike.com

marks, and may use the brands of third parties to identify their products and services.

***